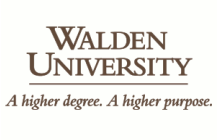
CORE
Metadata, citation and similar papers at core.ac.uk
Provided by Walden University



Walden University
ScholarWorks

Walden Dissertations and Doctoral Studies

Walden Dissertations and Doctoral Studies Collection

2018

Strategies Used by Cloud Security Managers to Implement Secure Access Methods

Eric Harmon
Walden University

Follow this and additional works at: https://scholarworks.waldenu.edu/dissertations


Part of the Databases and Information Systems Commons

This Dissertation is brought to you for free and open access by the Walden Dissertations and Doctoral Studies Collection at ScholarWorks. It has been accepted for inclusion in Walden Dissertations and Doctoral Studies by an authorized administrator of ScholarWorks. For more information, please contact ScholarWorks@waldenu.edu.

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Eric Harmon

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. Steven Case, Committee Chairperson, Information Technology Faculty
Dr. Timothy Perez, Committee Member, Information Technology Faculty
Dr. Michael Orsega, University Reviewer, Information Technology Faculty

Chief Academic Officer
Eric Riedel, Ph.D.

Walden University
2018

Abstract

Strategies Used by Cloud Security Managers to Implement Secure Access Methods

by

Eric Harmon

MS, Kaplan University, 2014

BS, Strayer University, 2012

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

December 2017

Abstract

Cloud computing can be used as a way to access services and resources for many organizations; however, hackers have created security concerns for users that incorporate cloud computing in their everyday functions. The purpose of this qualitative multiple case study was to explore strategies used by cloud security managers to implement secure access methods to protect data on the cloud infrastructure. The population for this study was cloud security managers employed by 2 medium size businesses in the Atlanta, Georgia metropolitan area and that have strategies to implement secure access methods to protect data on the cloud infrastructure. The technology acceptance model was used as the conceptual framework for the study. Data were collected from semi-structured interviews of 7 security managers and review of 21 archived documents that reflected security strategies from past security issues that occurred. Data analysis was performed using methodological triangulation and resulted in the identification of three major themes: implementing security policies, implementing strong authentication methods, and implementing strong access control methods. The findings from this research may contribute to positive social by decreasing customers' concerns regarding personal information that is stored on the cloud being compromised.

Strategies Used by Cloud Security Managers to Implement Secure Access Methods

by

Eric Harmon

MS, Kaplan University, 2014

BS, Strayer University, 2012

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

December 2017

Dedication

I dedicate this to my wife, Lawanda Harmon. The person that has supported me through this long process. Our journeys are not always easy, we may face difficulties; however, the prize for completion is self-fulfillment.

Acknowledgments

I acknowledge and thank all the following people for their involvement in this research:

My wife for putting up with my many hours that was needed for research and analyzing of data. I love you. Thank you for your support, understanding, and motivation.

All the individuals that took time out of their busy schedules to participate in my voluntary research. You time and participation was appreciated.

My committee chair, Dr. Steven Case, and all my committee members, Dr. Timothy Perez, and Dr. Michael Orsega. I would also like to thank Walden's chief academic officer Dr. Karlyn Barilovits and all staff members at Walden that I have worked with during these past years.

Table of Contents

List of Tables

List of Figures

Section 1: Foundation of the Study

Cloud computing is evolving and becoming a standard practice for storing, sharing, and accessing data with many end users and businesses. When companies choose to adopt the cloud computing technology, there is a change within information technology practices relating to how information is accessed, stored, and protected. With that adoption of a new technology, customers expect business leaders to protect sensitive data that is stored on their networks (Sauls & Gudigantala, 2013). It is vital that companies are able to prevent their networks from being breached and are able to manage network resources for building trust with consumers (Sauls & Gudigantala, 2013). While there are studies that discussed breaches on the cloud, there were few studies that addressed the safeguarding of the information from the security managers aspect in relation to network authorization. This study will address that gap in the research regarding securing data on the cloud network.

Background of the Problem

Companies experience a rise in cost due to keeping their cloud infrastructure safe from outside entities attempting to infiltrate their networks (Chen, Jin, Wen, & Leung, 2013). Cloud computing is becoming more common for information technology (IT) personnel at businesses because it provides an accessible option of storing and accessing data (Avram, 2014; Juels & Oprea, 2013). When companies invest in their IT group, they see an increase in the company's overall value (Avram, 2014); however, cost is still the initial discussion when organizations discuss changes and funding, even regarding providing needed security (Srinivasan, 2013). Cloud providers seek to reduce the risks

that occur on the cloud and increase the reliability of the infrastructure to establish a reciprocal trust between the cloud provider and the consumer. A survey conducted by Aleem and Sprott (2012) revealed that security, governance, and lack of availability to resources that were stored on the cloud was a major concern to corporations, and that data leakage was voted as a major threat to cloud computing in version 1.0 "Top Threats to Cloud Computing".

When companies choose to adopt the cloud, they open the user's ability to centrally store data and have access to it from any location (Avram, 2014). Researcher's opinions have varied regarding the security of cloud computing (Fernandez et al., 2014; Zardari, Jung, & Zakaria, 2014). Multiple researchers have documented concerns regarding security issues that exist with cloud computing (Fernandez et al., 2014). Breaches that occur on the cloud may affect items as minimal as pictures, or major items such as social security numbers, credit card information, or any PII (personally identifiable information) which could result in identity theft. In this study, I examined security issues that occur as it relates to cloud computing and the processes that some security managers have in place to protect information which they have stored on the cloud.

Problem Statement

Cloud computing can be used as a way of access services and resources for many organizations; however, hackers have created security concerns for users that incorporate cloud computing in their everyday functions (Fateminezhad & Soltanaghaei, 2016). Aleem and Sprott (2013) interviewed 2000 information and communication technology

(ICT) professionals and 93.4%stated their most significant concern with adopting the cloud was security. The general IT problem is that some cloud infrastructures have access vulnerabilities that affect securing data. The specific IT problem is that some cloud security managers lack strategies to implement secure access methods to protect data on the cloud infrastructure.

Purpose Statement

The purpose of this qualitative case study was to explore strategies used by cloud security managers to implement secure access methods to protect data on the cloud infrastructure. The population for this study was cloud security managers employed by two medium size businesses in the Atlanta, Georgia metropolitan area and that have strategies to implement secure access methods that protect data on the cloud infrastructure. The potential social impact of this study is the possibility of providing better cloud access practices, which may decrease security incidents that affect unauthorized access to people's private information by utilizing data that is obtained from cloud security managers that have implemented secure access methods.

Nature of the Study

I chose the qualitative method for my study. Researchers utilize a qualitative method to explore current concerns in detail and in depth (Lai, Tam, & Chan, 2012). Using the qualitative research method, I was able to obtain detailed information by performing one-on-one interviews using open-ended questions, which allowed free exchange of information, and provided value based off their experiences and knowledge regarding their current cloud security practices. The qualitative method was appropriate

for this research because my intent was to explore data that were collected regarding the current IT security processes that cloud security managers are using.

Quantitative research focuses on the probability and statistical components of data that are gathered (Goertz & Mahoney, 2013). A quantitative research method should have an original hypothesis that also includes how measured data will be utilized and how the hypothesis will be approved or disapproved (McCusker & Gunaydin, 2015). I did not design this study to either approve or disprove a hypothesis, so a quantitative methodology was not valid for this study.

When it is imperative to combine qualitative and quantitative methods, the researcher would want to implement a mixed-method approach (Venkatesh, Brown, & Bala, 2013). The mix-method approach would not be beneficial because the research question was able to be analyzed using the one research method, which was the qualitative research method. Neither the quantitative nor the mixed-method approach were appropriate for this study.

There are multiple qualitative method designs. Each research design provides various approaches that afford the researcher the ability to address the research questions that are formulated. The multiple case study method is appropriate when research is studying multiple cases to understand any similarities or differences between the cases (Stake,1995). The multiple case study was appropriate for my study because I performed detailed research on multiple cloud security managers employed at two medium size business using one-on-one interview questions.

Researchers use ethnography research designs to show how cultures react, social implications, or the communication between groups or individuals (Hoffman & Tarawalley, 2014). An ethnographic design was not appropriate for my study because I was not observing cultures or how groups reacted to security issues. A narrative research design is relevant when the researcher looks to explore the past experiences of their participant (White & Drew, 2011). The narrative design was not appropriate for this study because the life experiences were not the focus of this research. The phenomenological design is a philosophical approach regarding commonalities of people that experienced a particular phenomenon (Kafle, 2013). Because the focus of this research was not to look at the phenomenon of its participants, the phenomenological design would not be appropriate.

Qualitative Research Question

What strategies are used by cloud security managers to implement secure access methods to protect data on the cloud infrastructure?

Interview Questions

1. What strategies have you used to implement secure access methods to protect data on the cloud infrastructure?
2. What did you think was the deciding factors for implementing the current security methods over other security methods there are available?
3. Was there any training that you obtained that aided in your decision to suggest the current security measure that is in place?

4. Were there any concerns that you had regarding the adoption of the current security method?
5. Did you face any barriers when trying to implement the security policy?
6. In what ways do you feel that the current security policy that is in place is more beneficial than the prior process?
7. How well do you think others have accepted the security policy when it was implemented?
8. What processes do you have in place for training employees regarding security on the cloud?
9. Do you have anything else to add that I have not asked about security methods that you have implemented regarding the cloud?

Conceptual Framework

The conceptual framework that I used for this study was the technology acceptance model (TAM). Fred Davis (1986) developed the technology acceptance model to predict a user's acceptance of technology in the business world. The TAM assisted in identifying the relationship between perceived usefulness, perceived ease of use, features of the technology, usage behavior, and attitude toward using adopting the technology (Davis, 1986). After Davis's creation of the model, Bagozzi and Warshaw expanded upon theTAM to create a more efficient tool to identify user acceptance, to assist IT practitioners identify what issues users may have with adopting a new technology, and to create new strategies for a positive adoption rate (Bagozzi, Davis, &

Warshaw, 1992). The TAM may be one of the most prominent research models as it relates to the acceptance of information technology (Chau, 1996).

The TAM addresses the overall adoption process and addresses how inadequate learning of a technology may curtail its adoption. Bagozzi, Davis, and Warshaw (1992) used the TAM to help identify how perceived usefulness, perceived ease of use, features of the technology, usage behavior, and attitude controlled choosing the current security methods. Once the features of the current security methods were identified, those features were used to research the direct impact on the perceived ease of use and the perceived usefulness. Those perceptions will influence the user's attitude toward how the system may be used, and the user adopts the current security practices.

Definition of Terms

*Authentication.*Which is a method of verifying who a person is based off information that is provided. It's making sure that something or someone is who they claim to be (Aldwairi, Masri, Hassan, & ElBarachi, 2016).

Authorization. The process of verifying what permissions are granted to use what services and the method of verifying rights are granted for access to guarded data (Ranjith, Vijayachandra, Sagarika, & Prathusha, 2015).

Cloud computing. Which may also be called internet computing, that refers to a set of resources and services that have the ability of being accessed over the internet or on a network. Cloud computing is a model that enables on-demand network access to shared resources (Gupta, Laxmi, & Sharma, 2014).

Information Security. Refers to securing any information or data that is being stored and verifying that information is not able to be accessed in any unauthorized manner for fraudulent purposes (Bernik & Prislan, 2016).

Perceived ease of use. Perceived ease of use refers to a person believing that utilizing a certain technology would take minimal effort to accomplish a set task (Davis, 1989).

*Perceived usefulnes*s. Perceived usefulness can be defined as the level a person feels a technology may enhance his or her job performance (Davis, 1989).

Security Awareness. A method of making people aware of securing their computers and information they access while utilizing their computers. It also addresses the responsibility of the users with safeguarding the access requirements to gain the information (Alseadoon, Ramadan, & Khedr, 2016).

Technology Acceptance Model (TAM). The technology acceptance model is one of the main aspects of the technology acceptance model is its ability to provide and explanation of why technology may be accepted, the ability of explaining a user's behavior across a wide range of technologies, while still being theoretically justified (Davis, Bagozzi, & Warshaw, 1989).

Theory of Reasoned Action (TRA). The theory of reasoned action is one of the past persuasion models that was used in psychology. The model is used to identify the way a person adopts or their actual behavior could be determined based off their prior intention along with their beliefs of a given behavior (Fishbein & Ajzen, 1975).

Assumptions, Limitations, and Delimitations

Assumptions

Assumptions related to a research study are portions of information assumed to be valid for a theory to be tested (Foss & Hallberg, 2014). It was assumed that archived information that was collected regarding how breaches were detected and resolved at the small business were accurately collected and documented. I assumed that participants answered all interview questions honestly and based on personal experiences during the interview.

Limitations

Limitations can be described as anything that may be seen as a weakness regarding a study (Cunha & Miller, 2014). The first limitation referred to Yin's (2014) belief that some participants may respond to interview questions due to what they believed the researcher wanted to hear. The next limitation for this study was data collection was limited to medium size businesses in the Atlanta, Georgia metropolitan area that uses the cloud technology, which means that information obtained from data collection may not have the ability of being duplicated by performing research at other businesses. Using only security managers limited data in which the front entry level security technician may see, which is additional knowledge and data that can be provided to the study.

Delimitations

Delimitations are foreseen constraints that researchers use to clarify the results of a study (Sampson et al., 2014). The first delimitation is that I did not include medium size

businesses that are out of the Atlanta metropolitan area because that is outside of the area of my research. Another delimitation was focused on security managers that have been able to implement secure access methods on the cloud. The last delimitation of the study was the use of census sampling method to identify the participants of the study.

Significance of the Study

Consumer adoption of the cloud is dependent on how well the provider handles ethical and security issues that occur (Charlebois, Palmour, & Knoppers, 2016). This study may be informative to consumers regarding their information that is being accessed using the cloud technology. The study may also be valuable to cloud security managers that are unable to provide a secure environment for cloud users. Identifying security issues regarding accessing the cloud infrastructure may lead security managers to address security issues related to securing their cloud environment, and more secure methods for protecting consumer's data as it is stored on their infrastructure.

Contribution to Information Technology Practice

The gap in the body of knowledge regarding how consumers perceive the security and functionality on the cloud afforded the opportunity to address consumer's concerns regarding the cloud, and provide knowledge around cloud computing. I used this study to aide in the understanding regarding the underlying components of the cloud and how its use may affect security. By showing how some security managers can provide security through authentication, their methods showed evidence that the cloud can be a secure environment.

Implications for Social Change

This study will create social change by decreasing customers' concerns regarding information that is stored on the cloud. Many users do not understand how the cloud works or the process that is involved with them accessing information. Showing users that information can be safe while being stored at an offsite location should reflect a positive change. A positive change in a customer's mindset may decrease user's fear of their private data being compromised, which may increase cloud use.

A Review of the Professional and Academic Literature

My review of academic literature was conducted using ProQuest Central, ACM Digital Library, Science Direct, Google, Google Scholar, EBSCOhost, the Walden library, and various dissertations. Using Ulrich enabled the checking of all references in my study to verify they were peer reviewed articles. In-depth research allowed me to explore the current and past literature that is related to the conceptual framework, cloud security, cloud security awareness, cloud security governance, cloud security laws and regulations, and cloud authentication and authorization. I collected data and reviewed 68 sources pertaining to this literature review, 64 (94.1%) were peer reviewed articles, 58 (85.3%), and three seminal authors (4.35%).

The information in this literature review provided a scholarly foundation for my study and aided me in analyzing the current body of knowledge related to what strategies cloud security managers use to implement secure access methods to protect data on the cloud infrastructure. My review of literature has two major components, which are: security related to authorization and the TAM. To provide adequate information

regarding those components I subdivided the security and authorization categories into the following components: (a) cloud security, (b) cloud security awareness, (c) cloud security governance, (d) cloud security laws and regulations, and (e) cloud authentication and authorization.

The Early Seminal Works Theory of Reasoned Action (TRA)

The TAM, which was created in 1989 by Fred Davis, is an extension of the TRA created by Ajzen and Fishbein in 1975, and is one of the past persuasion models used by researchers in psychology (Ajzen & Fishbein, 1975). Using the TRA, Ajzen and Fishbein (1975) were able to associate a user's attitude and beliefs to their adoption of technology. Sheppard, Hartwick, and Warshaw (1988) believed that Ajzen and Fischbein's model proved validity when used within their defined restraints, regarding situations involving a choice problem not explicitly addressed, or the participants intentions are assessed when all information is not provided to them. However, researchers who wished to incorporate this model were interested how it would function when situations occurred outside of those constraints. The way a person chooses to adopt a technology or their behavior toward that technology could be determined based on their prior intention of the technology use, along with their beliefs regarding a given behavior (Ajzen & Fishbein, 1975; Mathieson, 1991). The Ajzen and Fishbein's model was used by researchers where (a) the participants did not have complete information to make a conclusive decision, (b) the participant did not have complete control of their behavior while being studied, and (c) issues that are related to certain choices not being available during the study were not addressed by Fishbein and Ajzen (Sheppard, Hartwick, & Warshaw, 1988). While the

TRA model was beneficial for certain trials, such as the test performed by Rutter (1989) to determine if there would be a significant difference in results if subjects were supplied with belief statements, compared to those subjects that we not provided any belief statements. Researcher use the TAM, which allows gathering of data without any form of result influence by using perceived usefulness (PU) and perceived ease of use (PEU) variables. The purpose of the TRA is "to model how any specified behavior under volitional control is produced by beliefs, attitudes, and intentions toward that behavior" (Hankins, French, Horne, 2000, p. 152).

Fishbein and Ajzen created models to measure behavior and attitude towards the intention to use something. While examing the origin of the TAM I researched how TRA was used to explore a users intention to use a product. The TRA used attitude and behavior while the TAM eplores the intention to use based on perceived ease of use (PEOU) and perceived usefulness (PU). In order to measure a subjects intention, Fishbein and Ajzen created created created equations, which incorporated variables to identify which factor was being used.

An equation used by Fishbein and Ajzen to measure behavior is represented by a B variable, and is predicted by their actual intention to perform based off that behavior, which is represented by variable I. The behavior is determined using the following equation B = I. Theory of reasoned action believes that a person's attitude toward performing a certain behavior is based off their intention to perform that given behavior, which is expressed by variable A, and based off what is considered normal in after

performing that behavior, which is represented by variable SN. The intention is determined using the I = A + SN equation.

Fishbein and Ajzen equation measures that a person's attitude toward a behavior is based on their beliefs of what the outcome will be from that behavior, which is represented by variable b, and the evaluation of that information represented by variable (Fishbein & Ajzen, 1975). Attitude can be defined as the affect that a person may associate with the actual use of a target system to perform their job (Fishbein & Ajzen, 1975, p. 216). Fishbein and Ajzen (1975) noted a persons belief regarding an object forms the attitude towards that object. Which allows attitudes to be measured by evaluating the beliefs.

Using the TRA, Ajzen and Fishbein (1975) suggested that a person's prior intentions, in addition to their beliefs, could have a direct effect on a person's actual behavior. The authors also suggested that an attitude a person has toward an actual behavior and the subjective norm could determine a person's behavioral intention. Even though researchers have used the TRA model across numerous studies it has had limitations when attempting to measure the acceptance of technology based on the PEU and PU variables.

The Early Seminal Works of theTechnology Acceptance Model

Davis (1989) used the TRA to create another model that used the behavioral intentional framework as a platform because it is useful for determining a user's intention of adopting a technology. While the TAM was based on the TRA, the model has advanced in several ways from the Fishbein model. The method in which the TAM

measures perceived ease of use and perceived usefulness differs from the Fishbein approach. The subjective norm variable that was used in the Fishbein model was not used in the TAM because there would be no information obtained regarding the assumptions of how other people are affected by the participants actions.

Fishbein and Ajzen (1975, p. 304) proposed that normative opinions can be formed in two ways. First, a person may be advised regarding what they should do by another party. Second, the person may come to a conclusion regarding their expectations based on information they receive or an observed event. In a normal acceptance test, participants used the technology for the first time, which did not give the participant the ability to receive any information from other users to establish a normative inference. Based on the user being unable to establish a normative inference (being advised of how they should respond by another party), the perceived social normative would not exist when the user performed testing. The results regarding acceptance are speculatory once those influences are removed, which researchers address when using the TAM when testing PEU perceived ease of use, and PU.

The TAM is a theoretical model that assesses the effects of system characteristics on user acceptance (Davis, 1985). Researchers have use the TAM in studies and it has been validated as an in-depth tool for explaining the adoption of IT by the users (Davis, 1989; Davis et al., 1989). There is a mutual relationship between predicted use, perceived usefulness, and perceived ease of use. Bogart and Wichadee (2015) revealed in their study that perceived usefulness and attitude had a positive effect toward the intention to use the LINE application, which aligns with Davis's reasons for creating the

TAM. The first change that Davis (1989) implemented was to omit the subjective normality construct that is included in the TRA action and the TPB. Davis suggested that individuals may choose to utilize technology to perform their jobs. The second change was regarding focusing on general beliefs, as they are related to the theory of planned behavior and theory of reasoned action. The TAM includes two additional key items that address beliefs that influence attitude and the intention to use technology: the PEU and PU of a technology.

The basis of the TAM is that researchers can use it to identify reasons why a technology will be adopted. One of the main aspects of the TAM is its ability to provide an explanation of why technology may be accepted (Davis, Bagozzi, & Warshaw, 1989; Sharma et al., 2016). The TAM is used to explore if users will adopt and utilize a technology based on the PEU and the PU. Perceived usefulness can be defined as the level a person feels a technology may enhance his or her job performance (Davis, 1989; Koufaris, 2002). The perceived ease of use refers to a person believing that utilizing a certain technology would take minimal effort to accomplish a set task (Davis, 1989). Lu, Liu, Yu, and Yao. (2014) stated that individuals evaluate the outcome of their behavior regarding perceived usefulness and base that behavior on their desirability of the perceived usefulness. Prior research has shown that perceived usefulness is used as one of the indicators for the showing the acceptance of technology acceptance (Persico, Manca, & Pozzi, 2014; Sharma et al., 2016). If the technology that is being offered does not help the individuals perform their job, the desirability of that product will not be high

Perceived ease of use may also influence a person's understanding about how using a certain system may increase their job performance. Dey (2013) stated that the perceived ease of use have a major influence on a user's decision to accept new technology. Within organizations, people may be rewarded for good performance in fashions such as promotions, bonuses, or raises (McKelvey & Pfeffer, 1984). Some users believe that a system that is high in perceived ease of use directly affects the effort needed to perform a task and should also have an equally high positive performance rating. Effort is a limited resource that someone delegates to activities in which they are involved (Radner and Rothschild, 1975). Utilizing the TAM aides in researchers using the variable perceived ease of use to determine its relevance to the adoption of a technology.

Davis (1986) developed the TAM was developed to provide validation regarding why users chose to accept a certain technology. Davis (1986) stated that he was developing the TAM with two major objectives in mind. First, to have an understanding of what the process was regarding users accepting new technology, and second, to state that the TAM should provide a theoretical basis for user acceptance testing which would enable software designers the ability of understanding how new systems would be used prior to its implementation. Being able to use the TAM required user acceptance testing. That would require creating a functional environment of the new technology, and having users use that environment, would allow the testing of the user's acceptance of a new system that was created (Davis, 1986). The creation of the TAM with the two identified objectives allowed Davis to further research users' acceptance of technology.

The success of technology implementation can be measured using two criteria: PEU and PU (Davis, 1989). Joo, Joung, Lim, and Lee (2015) used that same criteria to determine the factors that influence Facebook usage. Joo et al. (2015) used PEU and PU to determine its effect on how often a person chooses to use the Facebook application. Using the PEU and PU variables Joo et al. (2015) were able to create research questions to obtain data needed to understand why the Facebook application was being used by participants. By using the TAM, the researchers were able to provide validated data for the adoption of the Facebook application.

Researchers have used the TAM in several studies to determine what factors influence a user's acceptance of technology. The first factor is that people will use a technology based on how well it will assist them in performing their job, which is identified as PU. The second factor is, regardless of a user's perception that a technology is useful, they may feel it is difficult and may not see a benefit in using it; this is labeled as the PEU (Davis, 1989). PU and PEU is used in The TAM to create a understanding of why certain technology is used.

Studies Utilizing the TAM

Okundaye (2016) used the TAM to explain how external variables influence the belief, attitude, and the use of technology (Awiagh et., 2015; Wunnava, 2015). Okundaye (2016) used the TAM to explore how culture may influence the PEU the PU regarding the use of ICT. Using the TAM theoretical model (Okundaye, 2016) wanted to explore the predicted behavior toward using information and communication technology (ICT), where PU was one of the factors used to determine the use of the technology.

To explore the adoption of the ICT (Okundaye, 2016) used interview questions to collect data from the participants. Based on the response from those created questions, the author was provided insight regarding ICT adoption. From those 20 participants and the eight semi-structured interview questions (Okundaye, 2016) produced 32 codes which were used to identify commons themes in the collected data. To explore the reason for the adoption of the technology (Okundaye, 2016) created interviews questions to gain an understanding of why ICT was adopted. Each question addressed how the participant perceived the technology from their point of view and knowledge.

Cabral (2016), used the TAM to explore if PEU and PU were factors regarding the selection of projects. Utilizing the TAM Cabral (2016) wanted to explore the reasons why there was not a more structured process in place regarding the selection of projects. Using the TAM, Cabral (2016) sensitizing codes were created to analyze the recorded data. Those codes assisted the research in aligning the data with the supported theories. The author used 25 participants that were involved in the project selection process to explore the reasons why they choose those projects. Cabral (2016) used the interview questions to explore the participant's views on projects and their adoption. Using the TAM for the interview question creation, the author wanted to explore how the participants viewed the PEU and PU regarding the adoption of the project.

McIntosh (2017) used the TAM to explore why small real estate business (SREB) owners use certain strategies to implement cloud and mobility products to reduce technology cost. Looking to view how (PEU) and (PU) play its part in the strategies of implementing certain types of technologies to decrease cost. The qualitative research

method allows the researcher to dig deeper into understanding how, why, and what regarding this adoption. Which may benefit (SREB) owners to increase productivity and improve cost. The multiple case study allowed the researcher to reach data saturation by focusing on more than one corporation, which allowed information to be explored deeper.

The interview questions that were created allowed the author to explore information as it related to the research question. The author targeted the cloud and the mobility technologies, and each question was directed to that participant so it is not something that would have to be assumed, it is something that participants personally performed or thought. McIntosh (2017) conducted face to face interviews which allowed him to observe the participants behavior during that process to have a better understanding of why a certain decision was made. By transcribing and loading the interviews in NVivo, McIntosh (2017) could identify themes in the interviews, based on the emergent themes from those interviews, the researcher used NVivo to determine how many times those themes were talked about and which participants discussed it the most.

Studies Utilizing the TAM Regarding Learning Management Systems on the Cloud

To assess how users may reject or accept a technology, a researcher needs a method to measure the user's views. In this study Salas and Moller (2015) used the TAM, which was created by Davis (1989), to evaluate the adoption of a new e-learning application that was being stored on the cloud. Salas and Moller (2015) were exploring the faculty's PEU regarding the voice authoring tools. What are the faculty's PEU regarding the voice thread, and why would the voice thread be used? The TAM was used to show if there is a PU toward e-learning technology. Okantey and Addo (2016) utilized

the TAM as well to determine what factors influenced the adoption of e-learning at universities that were in various locations in Ghana and utilized cloud storage systems to house the e-learning applications.

Okantey and Addo (2016) adjusted the TAM model to utilize institutional factors. This was accomplished using a sample of 600 lecturers from both private and public institutions in Ghana, utilizing a correlation analysis to determine the relationship between institutional factors and e-learning adoption (Okantey & Addo, 2016). Salas and Moller (2015) obtained 10 faculty members for the study, which nine of them were female and one was male. To have diversity with the participants, there were five full time employees and five adjunct participants. While Ramírez-Correa, Arenas-Gaitán, and Rondán-Cataluña (2015), utilized the TAM to evaluate if students that were at different locations, where the universities utilized cloud technology, adopted the e-learning technology. The researchers examined the relationship between PEU and external controls to determine the adoption of the e-learning technology. When an academic institution is looking to implement a new technology, feedback regarding faculty's acceptance will show a value of that product. While all three studies utilized the TAM to determine the adoption of e-learning systems and applications that incorporate the cloud for its storage and access, they all utilized different tools to analyze the data and used different participant pools to gather information. The TAM two core indicators are good assessment tools to determine the impact of technology that's being introduced and related to the e-learning platform (Persico, Manca, & Pozzi, 2014). Researchers using the

TAM to determine why e-learning may be adopted has the ability of benefiting the provider and the user.

Securing the cloud technology brings into question the m-learning technology, which also expands a learning technology across numerous continents. Iqbal and Bhatti (2015) stated that the acceptance of m-learning depends on the attitudes of the participants utilizing that medium; therefore, this study focused on everyone's background, knowledge, and readiness regarding m-learning. Scholtz and Kapeso (2014) also utilized the TAM to evaluate the acceptance of m-learning and e-learning based on the PEU and PU. By utilizing questionnaires, Scholtz and Kapeso (2014) participants had to evaluate the systems they were completing tasks on, which related to the acceptance of technology based on the TAM. Shu-Sheng Liaw and Huang (2015), used surveys to determine the attitudes toward adopting the m-learning technology. The TAM is an ideal choice when investigating how users will accept a new technology due to its powerful nature, with the TAM being a strong research framework it was used as the basis for their framework (Iqbal & Bhatti, 2015). The TAM shows a compelling relationship between PU and PEU. Shu-Sheng Liaw and Huang used the TAM to determine the correlation of the perceived usefulness to the adoption of m-learning. When users find technology less complicated to use they will have a positive outlook for its usefulness (Iqbal & Bhatti, 2015). The connection between positive attitude and usefulness have been identified in several studies (Iqbal & Bhatti, 2015 as cited in Hu, Chau, Sheng & Tam, 1999; Bruner & Kumar, 2005). PU amd PEU play an integral piece in the acceptance of technology.

There have been several studies which correlate PEU and PU to a technology's adoption. Iqbal and Bhatti (2015) stated that in several TAM based studies that shows the direct effect of PEU and PU on behavior intention, which is the likelihood that a person will choose to use a certain technology. Iqbal and Bhatti (2015) used this approach to investigate factors that would affect the adoption of m-learning among university students and their ability to access the m-learning applications that are stored at other locations, and to determine if PU and PEU had a direct impact. Balavivekanandhan and Arulchelvan (2015) conducted a study to grasp an understanding how students felt regarding factors that influenced using m-learning technology. This study viewed students that were knowledgeable in IT to determine if they saw usefulness in this type of technology.

The study was conducted on 892 students that were in the Science, Engineering, and Art colleges. Asiimwe and Grönlund (2015) used online questionnaires to ask students questions to deem the PEUand PU regarding adopting the new technology. Based on the grouping of the questions the data received from the participants allowed the researcher to gauge those responses to determine that technology may be adopted. Balavivekanandhan and Arulchelvan (2015) believed that to determine the benefits of using mobile technology, the intent to use it would first have to be established. The TAM was used in this study to determine the PU and the PEU as it applied to the user and mobile technology. Researchers use the TAMin the technology world to grasp the concept of and the benefits that are obtained from its usage. All of studies were able to use the TAM as a tool to see if participants would adopt a technology if they felt the

technology was useful, if they saw a benefit in the technology, and the usability of the technology.

Studies Utilizing the TAM Regarding the Adoption of E-commerce Businesses on the Cloud

Due to a large increase of globalization of markets and retailing chains there is a need to understand how the TAM functions and how researchers using the model will assist in determining why users choose to adopt a technology. Ashraf, Narongsak, and Seigyoung (2014) utilized an extended version of the TAM to have a better understanding of how e-commerce is adopted across multiple cultures using online shopping. While Peiris, Kulkarni, and Mawatha (2015) performed a study on another cultural area adoption of e-commerce using the TAM. While the adoption of e-commerce may help smaller companies thrive, users still must see a need to use a technology. Ensuring transactions are encrypted, and clear information security policies are in place, improve e-shoppers trust in security (Lu, Chang, & Yu, 2013). Cross-cultural research has shown that consumers in different cultures have different expectations of e-retailer trustworthiness (Ashraf, Narongsak, & Seigyoung, 2014 as cited in Jarvenpaa, Tractinsky, & Saarinen 1999). Financial information is constantly being targeted while conducting transactions online.

For consumers to make an online purchase, a level of trust must exist between the purchaser and the merchant. This will have a major impact on the consumers' willingness to adopt the e-commerce technology (Peiris, Kulkarni, & Mawatha, 2015). In this study Ashraf, Narongsak, and Seigyoung (2014) used the TAM to clarify when and why PEU

and PU have an influence on the adoption of e-commerce. To achieve the objectives of the study two countries were chosen that are culturally different and at different stages regarding e-commerce (Ashraf, Narongsak, & Seigyoung 2014). To have a basis to measure the two countries on, the Computer Based Media Support Index (CMSI) was used, the Pakistan CMSI score is 261 and the CMSI score for Canada is 159. CMSI was developed as a means of expressing the simultaneous influence of all four dimensions on technology acceptance (Straub, Keil, & Brennan 1997). CMSI scores have been used to assist with predicting the adoption of e-commerce across countries, and the adoption of e-mail in countries such as Switzerland, Japan, and the United States (Straub, Keil, & Brennan 1997). Online shopping requires using technology, and with online shopping being a link between the consumer and the e-retailer, trust with the technology is a major factor.

While CMSI's are calculated summing the index scores of power distance, masculinity, and uncertainty avoidance, it does not factor the PEU and PU, which affects the acceptance of technology per the TAM. The model that was utilized incorporates trust and perceived behavioral control in a setting that is outside of the Unites States, which would provide a better understanding of why e-commerce is adopted outside of the United States. Peiris, Kulkarni, and Mawatha (2015) believes the main purpose of the TAM for their study is to predict the consumer's acceptance of technology. Predictions are made based on the system, needs, documentation, and training as it relates to factors that influence attitude and its acceptance.

Utilizing the cloud regarding enhancing the capability of e-commerce advances the development of business globally. Al-Bakri and Katsioloudes (2015) conducted a study that would explore factors that affected small and medium size businesses in Jordan adopting e-commerce technology by using a mixed method approach. The participants were chosen by using the Annual Handbook Index of 2012, which was compiled by the Jordanian Chamber of Commerce, from that list 500 participants in the industry were randomly selected. While Ashraf, Narongsak, and Seigyoung (2014) studied how e-commerce was being adopted across different cultures. While both studies utilized the TAM to determine why a technology was adopted, Al-Bakri and Katsioloudes (2015) looked at factors such as readiness, strategy, manager's perception, and external stakeholders, while Ashraf, Narongsak, and Seigyoung (2014) viewed the PEU, trust, and security practices. While Al-Bakri and Katsioloudes (2015) didn't identify security as being a component regarding the adoption of a technology, by identifying stakeholders as a factor, that may also be addressed in the study as well while using the TAM. Some researchers have used the TAM to hypothesizes that behavioral intention has a direct relation of attitude that PU and PEU together impacts a person’s attitude toward using technology (Davis, Bagozzi, & Warshaw 1989). The ability to understand the adoption of the e-commerce technology on the cloud by utilizing the TAM creates a strong foundation for implementation.

technology acceptance model Studies to Show the Adoption of EHR Systems that Store Data on the Cloud

The TAM addresses the overall adoption process, and have been used to determine the adoption of various information technologies. Esmaeilzadeh, Sambasivan, and Nezakati (2014) believed using technology in the health care sector would assist with improving performance of physicians; however, one of the main challenges regarding the usage of technology is getting the physicians to accept it. Johnson (2013) used the TAM to determine if registered nurse's attitudes toward the HIPAA security controls had any effect on their behavior to comply with the HIPAA security policies and procedures. The additional purpose of the study was to examine the correlations between access control technologies and the PEU, which is one of the main constructs of the TAM (Johnson, 2013). Akpabio (2013) performed a similar qualitative multiple case study where the TAM was used to determine the implementation of an electronic health record system. Johnson (2013) stated the findings from this study may assist in providing guidance to practitioners with developing or improving current access control methods that are in place that relate to PEU. Akpabio (2013) used this study to examine factors that aided the CIO to determine user's behavioral intentions regarding using a new technology, whereas in Johnson's study he was trying to address methods for improving access control.

The study that was performed by Akpabio, was conducted at three hospitals that were in the southeastern Florida area. Interviews were performed by representatives that were selected from each location. The interview questions that were asked allowed data to be collected regarding the CIO decision making process involving the adoption of an

interoperable EHR system. Johnson (2013) study would gauge how registered nurses voluntarily would either selected or not select the computer systems that were being used for this study. While the users had choices regarding if they would use a computer system or not, once they opted to use the system, they had no option of not using the access control methods in compliance with the security policies.

By having this study be non-volitional, participants had to use the access controls to access the information systems. One of the reasons Johnson (2013) chose this topic and used the TAM was to fill the gap regarding knowledge on information usage and its success. Understanding why individuals decide to use the new EHR system or reject it may assist CIO's in creating a format, or adjustments to the application that would influence their use. Akpabio (2013) used the TAM to view the factors that determined the user's behavioral intentions for using the new technology, which a user's intention may affect actual use. Akpabio (2013) used the TAM to research a specific genre of software and determine if it would be utilized and why it wouldn't be utilized, and if it wasn't utilized what issues needed to be addressed. The behavioral intention shows a direct impact on a person using a technology, which is a link to PEU and PU.

Cloud Security

While cloud security is a major issue for cloud computing, it is first important to understand what cloud computing is. Cloud computing provides a method of delivering computing resources (through a third-party provider) as a service to end users through applications, servers, and storage capabilities (Chou, 2013). Keeping data secure on the cloud is a key component when dealing with private and secure information. While

providing cloud services, the cloud service provider's goal is to ensure the data is safeguarded and to keep the data's integrity (Chou, 2013). The cloud computing services are comprised of three layers which are the system layer, platform layer, and application layer. The system layer (IaaS), provides its users the ability to services such as memory, storage, and network devices (Sharma, Gupta, & Laxmi, 2014). This service can be provided to users as an on-demand service using virtualization. The platform layer (PaaS) affords users the ability to create applications without having to purchase software development tools. PaaS gives clients more control over application management and development, which allows its users to migrate new applications with older software (Sharma, Gupta, & Laxmi, 2014). The application layer, known as the Software-as-a-Service (SaaS), allows users the ability to rent applications through a cloud provider. Renting the service gives users the ability of having access to applications that are stored at an offsite location (Chou, 2013). Having resources at an offsite location gives corporations a fail-safe option and decreases cost regarding spacing.

Security managers seek creative and innovated methods to identify current security issues and methods to repair issues. Security is a key requirement that needs to be considered for cloud computing (Singh & Pandey, 2013). Cloud computing security protects data from various threats and identifies vulnerabilities that may be on the network. It is important for customers to have an understanding regarding the levels of security that are being offered by the cloud providers (Srinivasan, 2013). During the periods where information is not available, damage may be done which may compromise the validity and confidentiality of that information (Singh & Pandey, 2013). Security

issues that occur on the cloud have the ability of being seen in two different views (Sen, 2013). The first view relates to how the service provider views the cloud service and the security methods they have in place to protect the data. The second view is regarding how the customer sees the service and believing the service they are using is secure enough to protect their data (Sen, 2013). Advancements in technology along with the innovation of various technological devices have created an increase of cloud utilization.

This increase of cloud utilization has created challenges for companies that want to use the service and keep data secure. There is not a one size fit all service that that works for any company or users that choose to implement cloud technology (Rong, Nguyen, & Jaatun, 2013). Companies must attempt to tailor the service for it to work for the users and provide the necessary securities. It is important for security managers to implement security methods to protect stored data against security threats (Kumar, Jain, & Barwal, 2014). Security of data must be at the forefront of any security plan for information to be protected. For information to be protected on the cloud it is imperative for security managers to understand the importance of information that is being stored and the fundamentals of securing information. To ensure data security, key elements should be addressed which are encryption, decryption, key management, and access control (Wei, Zhu, Cao, Dong, Jia, Chen, & Vasilakos, 2014). Security on the cloud will not just stop with creating security methods, to oversee information security methods must be maintained to keep constant security. Cloud computing security is a set of policies that adhere to rules that are regulated to protect information, the data infrastructure and applications (Mishra, Mathur, Jain, & Rathore, 2013). Sen (2013),

stated there are numerous security issues with information regarding cloud computing because it encompasses various technologies, which incorporate databases, virtualization, networks, and operating systems. Sen (2013) also stated that security issues for many technologies will apply to cloud computing. Networks that combine systems in cloud computing should be secured to protect data; however, when connecting systems that are in various locations are interconnected it can lead to several security concerns (Sen, 2013). Further, Sen noted that security issues for many technologies will apply to cloud computing.

Viewing what a user plans to accomplish by using the cloud may provide insight on what their expectation is regarding the cloud's security. Kshetri (2013) performed research to analyze how the characteristics of the cloud have an effect on its security and its privacy. Cloud providers have the ability of providing low cost security options; however, cheaper security may lead to additional vulnerabilities (Kshetri, 2013). Kshetri (2013) stated the cloud is vulnerable when there are criminal owned clouds that are run in parallel with a valid cloud platform, which means the criminal-owned cloud would be able to effectively steal information. From the user's viewpoint, they are dependent on the vendor to provide valid security practices to safeguard their information. Users of the cloud have no access to the hardware or any of the resources that physically influence the cloud, which places the cloud provider as the primary security source (Kshetri, 2013). When the cloud provided is being determined the primary security resource regarding the data that is being stored, the consumer looks to the provider for answers when issues may occur.

Users view storing applications on the cloud as beneficial due to its ease of access and its expansion abilities: however, with the migration of applications there are concerns that consumers may not be aware of. Andrikopoulos, Binz, Leymann, and Strauch (2013) research was regarding moving applications over to the cloud environment, which also addressed what challenges are faced when customers attempt to move information over to the cloud platform. This issue is addressing using virtualization and deployment to the cloud, as well as delegating the adaption over to the cloud based on the current level of resource management. During the research Andrikopoulos et al., (2013) addressed what type of applications would be migrated, the effect of the migration, and the pros and cons of the migration. One of the identified issues was confidentiality, which involved avoiding confidential data being obtained, which relates to security and privacy. Regarding confidentiality, being able to keep data private and secure is paramount for the cloud provider, customer, and companies (Andrikopoulos et al., 2013). Confidentiality or the lack thereof affects the credibility of the cloud infrastructure, which leads to concerns when applications are migrated over to the cloud.

Users being concerned regarding threats occurring on the cloud can be a concern for the consumer and the provider. Nicho and Hendy (2013) completed a study to determine threats that were occurring from people utilizing the cloud technology. Nicho and Hendy wanted to identify the reasons behind the threats that were occurring by comparing issues that have occurred on the cloud infrastructure from past literature that was available. Based on present metrics of security threats Revoredo da Silva, Costa da Silva, Rodrigues, Medeiros Campos, Marques do Nascimento, & Cardoso Garcia (2013)

identified seven security threats that exist regarding cloud computing, those threats are: Abuse and Nefarious Use of Cloud Computing,

Insecure Interfaces and APIs, Malicious Insiders, Shared Technology Issues, Data Loss or Leakage, Account or Service Hijacking, and Unknown Risk Profile. While Nicho and Hendy (2013) research was attempting to identify reasons behind threats Revoredo da Silva et al., (2013) described seven threats from research questions. Based on the information that Nicho and Hendy (2013) could locate they would explore the different dimensions to determine the nature of the threats by performing interviews with cloud computing practitioners that work in organizations that use public and private cloud deployment models. In the research Nicho and Hendy (2013) identified there was a growing trend of adopting cloud computing by organizations; however, there is an increase in issues regarding security. Nicho and Hendy (2013) stated that even with numerous issues with cloud computing being researched from different perspectives, there is no clear definition of what's considered to be a threat. Due to the limited research that has been conducted to label what is considered to be a cloud security threat, a means of classifying of security threats are lacking (Nicho & Hendy, 2013). While users identify the cloud as being beneficial, the fear of threats that may affect their information could be a deterrent.

Having knowledge that security issues exists may cause technicians to address those issues when performing security testing on the cloud infrastructure. Kalloniatis, Mouratidis, and Islam (2013) performed research regarding cloud deployment scenarios regarding security and privacy issues that occur. Kalloniatis et al,, (2013) stated there

have been no research that has been done regarding security and privacy requirements, and no information as it relates to the cloud deployment model. There have been research that addressed security issues; however, it has failed to direct attention to the framework. While Kalloniatis et al., (2013) understand there are security issues that occur on the cloud, the issue of the framework needed to be addressed prior to just identifying there is a security problem. Kalloniatis et al., (2013) research was to propose detailed security and privacy requirements regarding the framework which addressed the selection process for the deployment model. The model in which they created provided a modeling language that incorporates security and privacy requirements which affect the information on the cloud framework.

Cloud Security Awareness

A common issue that occurs with securing the cloud is that many security managers will focus only on the technical controls. It is important to understand that minor mistakes that occur on the cloud network may have a large impact on the job of the security manager to protect stored data (Donald, Oli, & Arockiam, 2013). Security is controlled through awareness of issues and can occur without a proper understanding of how security works. Security awareness requires a complete solution to all systems that are involved, which incorporates policies and expertise (Donald, Oli, & Arockiam, 2013). The protection of data on the cloud has become a major issue for the provider and the consumer, which makes keeping data secured a major priority for security managers. Therefore, non-technical threats should also be considered when cloud security awareness is being addressed. Stanciu and Tinca (2016) stated there is a gap between

company's actual awareness of security issues regarding information technology and actions that are taken to resolve those issues. Actions regarding security issues will have a large impact on the success of policies that are being implemented.

Companies have the ability of enforcing policies that are adequate; however, if employees are not trained regarding new policies, and they do not understand the need of awareness regarding IT risks, companies still remain less protected (Stanciu & Tinca, 2016). Kim (2013) stated individuals need to be periodically measured to determine their current knowledge regarding security awareness. Information security should be considered a primary issue when trying to protect information stored on a network (Kim, 2013). Kim (2013) stated prior research has shown that individuals may have knowledge regarding technology; however, their security awareness is minimal which affects the protection of assets. The importance of security awareness is proved time and time again by the breaches that occur on the cloud (Allam & Flowerday, 2014). Security managers play a vital role with ensuring the implementation of policies and procedures regarding information security strategies. Security managers must maintain creative strategies to protect assets within the organization (Aleem, Wakefield, & Button, 2013). Security managers play a vital role with ensuring the implementation of policies and procedures regarding information security strategies.

Security managers have a constant concern regarding security awareness. Misenheimer (2014) conducted a study to examine security needs and requirements of universities and colleges, based on information provided regarding those security needs. Administrators may have the ability to address potential security attacks, threats, or

breaches. Ngoqo and Flowerday (2015) study related to existing practices regarding security and its poor implementation rto information security. This study was to identify factors to contribute with improving information security to reduce attacks, breaches, and threats within colleges and universities. In this study Misenheimer (2014) used IT personnel participants from colleges and universities throughout the North Carolina area. Misenheimer (2014) obtained participants from community colleges, public and private colleges and universities that offered degrees in the associate, bachelor, masters, and doctoral disciplines. The participant list involved 13 individuals from 12 separate institutions. The participants that Ngoqo and Flowerday (2015) used in their study were from a comprehensive university structure that was formed in 2005, which was from three merging historically black institutions. Ngoqo and Flowerday (2015) utilized behavior intent to determine why students chose to use security methods or decide against using them. While Misenheimer (2014) utilized the Complexity Leadership Theory (CLT), which is a bottom up approach, assist management in designing secure information systems based on what the system needs and what the technology requires. Due to the large amount of intrusions that occur on the cloud infrastructure daily, along with the increased threats that affect business assets, security managers need security measures, such as awareness to protect their company's assets.

Cloud Security Governance

Cloud security governance can be defined as a general method of creating and applying specific policies to the use of cloud computing services, also seen as guidance for enterprises to achieve security goals (Hung, Hwang, & Liu, 2013). Being able to

protect the cloud network is an instrumental part of securing user's data. Hung et al., (2013) one of the primary goals of cloud governance is the ability of securing data when it is located at a remote location. Al-Rashedi (2014) believed an important factor regarding the governance of cloud security, is being able to address concerns related to protecting information stored on the cloud due to lack of knowledge. Security governance ensures that IT assets are used according to all policies that are created and all assets are properly used (Sareen, 2013). IT governance should also include polices that control and measure how systems are being managed (Sareen, 2013). Cloud security governance is not solely related to technology, it relates to organizational issues and how individuals work together to establish business goals. It is important to establish the best practices for monitoring the created processes. Governance of technology establishes a direction of data security with the cloud (Hung et al., 2013). The organization of the cloud network and how the network is managed plays a large part in the success of security on the cloud

The effectiveness of information security governance can be examined by the organizations capabilities, belief actions, and their behaviors. Security governance allows security managers a basis for creating security policies, and once created they will be able to implement those methods which provides a means of protecting information assets (Whitman & Mattord, 2014). Matrane, Talea, Okar, and Talea (2015), believes that for a company to achieve information economy and security on the cloud, governance of IT is critical. Security governance can be a complex component for many security managers because it involves creating risk management policies that compliments its business needs (Yaokumah, 2014). Security governance is an imperative component for keeping

data safe within the cloud infrastructure. To have a strong security governance program it is important for any risks to be identified and assessed; this includes technical and non-technical issues (Yaokumah, 2014). The more that security managers and users understand regarding security risks exist the easier it will be for a security governance programs to be implemented. A well thought out security governance plan allows security managers to have more control of how security is implemented and what users are included in its implementation, while the security governance plan should be flexible to make adjustments for changes in technology, it must be static enough to keep the network safe.

When attempting to plan for an information security governance policy, security managers must provide a means to show its value, how will it benefit the company and will it work for the current budget (Whitman & Mattord, 2014)? While attempting to develop any type of security policy it is important for security managers to mitigate security risks to create an effective method to effectively implement those policies. With the increased usage of cloud computing and the types of devices that can be used to access the cloud it is imperative to create and incorporate an effective security governance program (Akintomide, 2013). This would also mean security managers must create a policy that is flexible and can be changed on the fly. When policies are being constantly changed and there is not a strong framework to refer to, security managers run the risks of opening a network up to security breaches. Mishra (2015), stated security governance describes how information security policies should be created and implemented within an organization. Creating an understanding regarding the need of

having a security governance policy will show the benefits of investing in a security governance program, which should ensure effective security controls (Mishra, 2015). Security leaders within organizations understand that having an effective security governance policy in place will have a direct relation to securing the confidentiality, the integrity, and availability of information assets.

Cloud Security Laws and Regulations

The implementation of cloud computing has been a beneficial and fearful process for many people and businesses. With cloud computing being a service that can be accessed globally there are policies, laws, and regulations that are created and enforced by the government officials, failure to comply to those regulations could result in legal issues (Dove, Joly, Tassé, Burton, Chisholm, Fortier, & Kent, 2014). With policies and laws created, this creates a foundation for the cloud computing framework, which will also have a direct impact on the minimal security policies that must be established. Regulations that have been created include, but are not limited to Family Educational Rights and Privacy Act (FERPA), ECPA (Electronic Communications Privacy Act), and Fair Credit Reporting Act, the Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley Act (SOX), and Gramm-Leach-Bliley Act (GLBA) (Srinivasan, 2013). Information that is stored by either a business or an individual using a cloud service provider may have less security that when users store their data themselves (Srinivasan, 2013). Srinivasan (2013) stated the main purpose of this report is to raise awareness to customers that utilize the cloud regarding security and privacy concerns.

The standardization of rules and regulations that are created by nations become a framework for nations that are underdeveloped.

The way that cloud service providers handle access to private data that is stored on the cloud, relates to the regulations regarding the physical security of data that is stored within their network (Srinivasan, 2013). It is important for cloud service providers to be knowledgeable regarding regulatory and legal requirements that are necessary when dealing with private data that would be stored in a cloud network (Adjei, 2015). Legal requirements may change based on the data being stored locally or if the data may be located internationally, those legal issues and requirements must also address any contractual obligations that are documented and defined (Adjei, 2015). Regulations also refer to the cloud framework which should address issues such as vulnerable systems not being deployed, which affects stored data, and cloud resources are utilized for legitimate purposes only (Adjei, 2015). Cloud computing can lack adequate guidelines for proper management of privacy guidelines and security, which may be related to laws and guidelines being different based on the country where the cloud is being housed (Adjei, 2015). Having laws and guidelines in place to provide a secure cloud environment provides a strong foundation for keeping information safe; however, it will only be beneficial if implemented correctly.

Cloud Authentication and Authorization

Confidentiality of information that is stored on the cloud is of major importantance regarding security. Ranjith, Vijayachandra, Sagarika, & Prathusha (2015) stated that confidentiality of data that is stored on the cloud needs to have the ability of

preventing unauthorized disclosure of data that is being accessed or that's in a rested state. When users attempt to access the cloud network they are authenticating their information, which is the process of identifying who they are, once that information is authenticated the user will be authorized to access the cloud network, which says what your permissions are once on the network (Ranjith et al, 2015; Stoetzer, 2016). Thomas, Dhole, & Chandrasekaran (2015) discussed using a single sign on option to access multiple systems as a means of authentication. The authentication step for the cloud network is important because it states who the person is based on the information which is provided. Abdellaoui, Khamlichi, & Chaoui (2016) proposed adding an extra level of authentication on the cloud, which is an additional form of security. The process will create a registration step in which the users must complete to access the cloud, if the users attempt to login to the cloud without registering they will be redirected back to complete that step (Abdellaoui et al., 2016). The registration step creates an additional security step regarding protection.

Once the user goes to login, the server will be able to compare the username and password that is stored in the database to what the user has input, if the data is correct the user will be granted access. Abdellaoui et al., (2016) explain how this process differs from other methods because there will be a AuthModule installed on the device the user has which provides an image to the user, that secret image will be validated each time the user attempts to gain access. If that image from the AuthModule application is not verified along with the username and password, the user will not have access. Ghazizadeh, Zamani, Jamalul-lail, and Alizadeh (2014) used a different type of method

for authentication which was single sign-on (SSO) that was introduced to combat security issues on the cloud. One of the main attacks that occur when users attempt to authenticate, which is the man in the middle attack, can be withstood with this form of verification because the password can only be valid for only one authentication session (Abdellaoui et al., 2016). With many users having multiple email addresses and login accounts, man in the middle attacks can easily occur when users having multiple accounts in which they must login to which occurs multiple times a day (Ghazizadeh et al., 2014). Abdellaoui et al., (2016) proposed the authentication method regarding registration as an optimal method which should increase security on the cloud platform. Ghazizadeh et al., (2014) stated SSO has a major role as it applies to cloud security, utilizing SSO can assist in improving security and privacy issues (Stoetzer, 2016). Thomas, Dhole, & Chandrasekaran (2015) agrees with using SSO as a means of protecting login credentials by allowing requiring logging in once and having access to all resources. There have been several studies that have been done to determine optimal methods for authorization and authentication, which show the there is an issue with authentication; however, finding the best method to secure information is still a difficult task.

In summary security managers continue to find new ways to increase security on the cloud to protect their client's information. There is always a need to find the best practice that is feasible for the business and the consumer, which reduces risks and cost when possible. For cloud resources to be secured it is important for companies to implement multiple sources of security, which also relates to educating the cloud provider as well as the consumer. Having proper training and support from upper

management allows IT security managers better resources when trying to create better security options.

Gap in Literature

While there has been a significant amount of studies that have been performed regarding cloud computing and security issues regarding cloud technology because its creation, there has been a lack of research that revolved around security issues that are related to secure access methods as it relates to protecting data on the cloud infrastructure. With there being a limited amount of professional published literature regarding secure access methods and their security concerns as they relate to the cloud infrastructure, I am completing a qualitative single case study focused on addressing and highlighting information as it applies to security issues as they relate to access methods on the cloud. While using multiple research databases (i.e., Science direct, ProQuest, Ebsco) and to investigate security issues as they relate to secure access methods, there were no results related directly to securing the cloud infrastructure by using secure access methods. While not being able to find my direct study presented and issues finding documentation to support my study, I was able to locate information as it pertained to the cloud infrastructure, and security breaches that have occurred on the cloud. That alone showed where there is a lack of information as it related to my topic.

Gap Chart from Prior Research

Table 1

Author/Date	Access Methods discussed	Identified Security Issues	Significant Findings
Andrikopoulos, Binz, Leymann, &	No	Yes	Discussed migration of resources over to

Strauch/2013			the cloud. An issue that was identified was confidentiality of information during the migration
Kalloniatis, Mouratidis, & Islam/2013	No	Yes	Stated research has been done regarding security; however, none relates to the framework
Ngoqo & Flowerday /2015	No	Yes	Even though students knew there may be security issues, due to their behavior of using the technology they were not concerned with security.
Misenheimer/2014	No	Yes	Looked at securing the cloud form the standpoint of what the system needs using a bottom up approach

The authors in (Table 1) have performed extensive research on security issues that relate to cloud computing. While their studies address security issues that relate to the cloud they fail to address issues that relate to authentication and authorization of users on the cloud infrastructure. Kalloniatis et al., (2013) identified there is an issue regarding security on the cloud; however, they relate it to being an infrastructure issue. Andrikopoulos et al., (2013) identified a similar issue and related it to the issue occurring during the migration of information over to the cloud and not addressing the security failures once the system is in place. While Misenheimer (2014) research identified the cloud was being secured based off the needs of the system, which does not address the

authorization standpoint. Ngoqo and Flowerday (2015) research addressed security from the standpoint of users knowing there is an issue; however, due to what they wanted to use it for they were not concerned. Being able to locate peer reviewed articles that showed there were issues related to security would allow me to use those articles to address the gap in the literature. My research will address the issues regarding security issues on the cloud infrastructure that relates to the correct users having the correct access and permissions to access resources, and by having access without those permissions, there being a security vulnerability.

Transition and Summary

Section 1 included an introduction of the proposed study which addressed the problem; which is that some cloud security managers lack strategies to implement secure access methods to protect data on the cloud infrastructure. With Section 1 there was also information regarding the purpose of the study, its significance, the nature of the study, and the population that would be researched in this study. The literature within Section 1 encompassed data regarding studies related to access vulnerabilities while utilizing the cloud infrastructure, issues that have occurred due to inappropriate security methods, and various studies that have utilized the technology acceptance model to validate the acceptance of the cloud technology. The data that was presented in the literature review showed a gap in research and validated the need for this study, which will assist in the understanding regarding the underlying components of the cloud and how it affects security. Section 2 (The Project) will begin with an introduction that provides an outline of what this section will include. The overall purpose of Section 2 is to provide readers an

understanding of the study and what is being researched. In Section 2 the purpose of the study will be discussed, describe the role of the researcher, the participants in the study, how the information will be collected and what instruments will be used. Within Section 2 the methodology will be discussed and the justification regarding why the methodology was chosen will be addressed. In Section 2 the steps used to ensure research was performed in an ethical fashion will also be discussed.

Section 2: The Project

A qualitative single case study approach was appropriate for this research because my intent was to explore data that is collected regarding the current IT security processes that cloud security managers are using. Section 2 includes the purpose of this study, a discussion related to the role of the researcher, an explanation of the participants, the research method and design, the population and sampling, and ethical research. Section 2 also includes the data collection methods, data collection techniques, data instruments, and data analysis. The end of Section 2 includes a discussion of reliability and validity of data.

Purpose Statement

The purpose of this qualitative case study was to explore strategies used by cloud security managers to implement secure access methods to protect data on the cloud infrastructure. The population for this study was cloud security managers employed by a medium size business in the Atlanta, Georgia metropolitan area that have implemented secure access methods that protect data on the cloud infrastructure. I performed the data collection process by interviewing cloud security managers that have been in the industry for at least 5 years and have had experience using and supporting the cloud platform. The potential social impact of this study is the possibility of providing better cloud access practices, which may decrease security incidents that affect unauthorized access to people's private information by using data that is obtained from cloud security managers that have implemented secure access methods.

Role of the Researcher

One of the researcher's goals when performing research is to gather quality data. When performing a qualitative case study, the researcher will gather information from multiple sources, such as interviews, archived data, documentation, observations, and current records (Yin, 2014). The researcher is the primary individual that collects the data and makes sense of the information that is collected objectively (Tomkinson, 2015). My role as the researcher in the data collection process of this qualitative single case study was to function as the primary data collection instrument, which allowed me to organize and interpret the data. While gathering data through interviews and archived data I, functioning as the researcher, did not have a bias as to how the information was interpreted, or the type of archived data that was collected. My role in this study was to obtain participants, conduct interviews, and collect and analyze data.

It is the researcher's responsibility to take the necessary steps to mitigate any biases that could occur and may affect the information that is being collected and analyzed (Fusch & Ness, 2015). When researchers are the primary data collection instrument they may find it difficult to control their biases when interviewing participants (Roulston & Shelton, 2015). My past and current work experiences have been in the IT field and dealt largely with security as it relates to networking. Dealing with network security and the breaches that have occurred on several networks led me to this study, to dive deeper into how security issues occur on the cloud infrastructure. My past experiences did not affect my objectivity during the interview process.

To mitigate biases during the interview process, I did not use interview questions that swayed the responses in any one direction. Once the interview questions were analyzed and verified, I presented the information as stated, and did not misinterpret any information. I reviewed the Belmont Report which is a summary of ethical guidelines and principles that protects human subjects in research (Belmont Report, 1979). The Belmont Report is a report that was created by the National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research and was published in the Federal Register in April of 1979 (Belmont Report, 1979). The Report addresses consent, privacy, anonymity, and protection of information obtained from human participants.

I presented the participants with consent forms that stated they were free to opt out of the study at any time. I protected participant privacy by not sharing their names with other participants or using their names in the study. All information that I obtained was kept secured during all times to protect participants' information. I used interviews to gather information from participants. Using an interview protocol allows research to use standardized interview questions that will provide consistency and allows the process to be consistently repeated if necessary (Gioia, Corley, & Hamilton, 2013). I used an interview protocol (see Appendix A) to provide a guideline to ensure all participants were asked the same questions and treated fairly.

Participants

Researchers must determine the criteria to select participants that meet the requirements for the study, which enables other researchers the ability to validate the

information that was obtained (Elo et al., 2014). The participants that I used for this study were cloud security managers that are employed at medium size businesses in the Atlanta metropolitan area and have strategies to implement secure access methods to protect data on the cloud infrastructure. The participants for this study were assigned to CSIRT (Computer Security Incident Response Team). The (CSIRT) allows qualified individuals to be involved with issues as they occur and responding to security issues to work toward the resolution (Wara & Singh, 2015). Participants that have used the cloud service for accessing resources, storing data, and securing information that is being stored on the cloud, was beneficial for this study.

By using a knowledgeable and experienced participant base, information will be related to security and methods that are taken to control it (Inan, Namin, Pogrund, & Jones, 2016). The participants in this study have been able to implement secure access methods to protect data on the cloud infrastructure. These participants also played a vital role with keeping the security policies updated and enforced in the cloud infrastructure.

Gioia, Corley, and Hamilton (2013) suggested there should be a standardized accessibility process when obtaining participants for any type of study. To gain access to participants I reached out to medium size businesses operating within the geographical boundaries of the Atlanta metropolitan area that support the cloud infrastructure.

Once I obtained authorization from the corporation, I obtained an email distribution list from the authorizing representative. The email distribution list that I obtained only pertained to individuals that support the cloud infrastructure. Once I obtained the email distribution, I was able to send out emails to participants advising

them of the study and gaining permission for them to participate individually. I used the letter of cooperation to obtain approval from the medium size technology business to conduct interviews with cloud security managers. Once I obtained approval from the Institutional Review Board (IRB) the letter of invitation (see Appendix B) was emailed to security managers to participate in the interview process. Based on the participants willingness to participate, I reviewed the consent form with participants prior to the interviews occurring. The consent form included an outline of the confidentiality that is associated with participating in this research study. Furthermore, the consent form included information that the participants have the right to withdraw from the research study at any time for any reason.

Creating a comfort zone with participants may cause participants to be more relaxed during an interview and provide more valuable information. When participants trust the interviewer a rapport will be established (McDermid, Peters, Jackson, & Daly, 2014). The participants were interviewed face-to-face using open ended questions, which allowed the participants to have direct contact with me. Using this interview method allowed me to build rapport with the participants.

When participants feel comfortable with the interviewer, and in a comfortable environment, the interviewer may receive more in depth responses (Yin, 2014). I conduted interviews at the participants employed location, in a private room, which allowed them to speak without restriction, this served as a comfortable environment for the participants. Having general discussion with the participants prior to the actual interview increases trust (Patton, 2015). To build trust with the interviewee, I started the

interview with general conversation, asking the interviewee how their day was going. By creating general conversations and not bombarding the participants with questions initially, I created a relaxed environment.

Research Method and Design

Research can be conducted utilizing three research methods: qualitative, quantitative, and mixed method. Each method has benefits and drawbacks. The design that a researcher uses is based on what the researcher chooses as their researcher method.

Method

I used a qualitative research method to explore the strategies that security managers at a medium size business in the Atlanta metropolitan use to implement secure access methods. Researchers utilize a qualitative method to explore current concerns in detail and in depth (Lai, Tam, & Chan, 2012). Qualitative research can be defined as a methodical collection, organization, and interpretation of textual information that may be obtained from any form of conversation (Grossoehme, 2014).

As I conduct interviews, I separated all data that I collected based on from whom it was obtained. For archived data, I separated them by year and importance. Qualitative research can be just collecting data from a single participant if they are from a single case study (Risk, 2013), or a group of participants if a large group of people are affected by the same issue (Grossoehme et al., 2013). For my study, I collected data from two different corporations to examine the issue from different business perspectives. By collecting data from multiple participants that have secure access methods in place, I was

able to obtain in-depth information regarding processes used to secure access to the instructure.

Using a qualitative research method, a researcher can explore the issues more in depth by asking the participants how and why questions related to the subject matter (Bailey, 2014; Ali & Cullinane, 2014). I was able to obtain detailed information by performing one-on-one interviews using open-ended questions, which allowed free exchange of information, and provided value based off their experiences and knowledge regarding their current cloud security practices. Researchers who use other research methods may not uncover a deeper or broader understanding in the same fashion as those using a qualitative method (Levy, 2015).

There are two other methodologies that I could have used for my research: quantitative and the mixed-methods. Quantitative research focuses on the probability and statistical components of data that is gathered (Goertz & Mahoney, 2013). A quantitative research method should have an original hypothesis, which will also include how measured data will be utilized and how the hypothesis will be approved or disproved (McCusker & Gunaydin, 2015). This study was not designed to either approve or disprove a hypothesis, so a quantitative methodology was not valid for this study. Quantitative research incorporates the use of regression tests to create an understanding of a relationship between dependent and independent variables (Tai, 2015). Quantitative researchers collect and analyze information to establish a conclusion that is based from statistical evidence that is collected to test a theory or a hypothesis (Trafimow, 2014). My study does not address a relationship dependence between variables to explain

technology acceptance. This study is not designed to test a theory, so a quantitative methodology is not valid for this study.

The mix-method approach would not be beneficial because the research question was able to be analyzed using the one research method, which was the qualitative research method. The mixed method approach is designed to incorporate both the quantitative and qualitative methodology into one study (Kipo, 2013). The mixed method approach was ruled out of my study due to it requiring both the qualitative and quantitative method to collect information and that was not needed for my study. Utilizing a mixed method approach researchers can combine data that is obtained by researching specific variables and experiences that is obtained from participants (Yin, 2013). When it is imperative to combine two methods, the researcher would want to implement a mixed-method approach (Venkatesh, Brown, & Bala, 2013). Therefore, the quantitative and the mixed-method approach were not appropriate for this study.

Research Design

Each research design provides various approaches that will afford the researcher the ability to address the research questions that are formulated. The multiple case study method will allow multiple cases to be explored and to allow for variations to be identified (Stake, 1995). Using a multiple case study design, I was able to gather and analyze data from multiple corporations and analyzed the experiences from the participants involved. A case study allows issues to be explored, which requires data to be collected from multiple data sources (Yin, 2014). The multiple case study was appropriate for my study because I performed detailed research regarding their security

methods on multiple cloud security managers within two medium size business using one-on-one interview questions.

When utilizing a case study, it may be ideal to collect data from at least two of the following six sources: (a) interviews (b) site visits (c) documentation (d) participant observations (e) archival records, and (f) physical artifacts (Yin, 2014). A researcher collecting data from multiple sources increases their credibility and adds credibility to the conclusions reached in the study (Houghton, Casey, Shaw, & Murphy, 2013). I collected and analyzed information from two different corporations which showed how different companies resolve security issues. Interviewing participants creates an environment of open communication between the participant and the researcher (Anyan, 2013). I performed face-to-face interviews which allowed for open communication which led to additional pertinent information regarding their security methods being obtained. Utilizing archived data such as recordings and documents provide valuable qualitative research data (Langen et al., 2014). Archived data being analyzed in conjunction with interviews by the researcher has the ability of identifying research themes (Lee et al., 2014). Utilizing archived data such as recordings and documents provide valuable qualitative research data (Langen et al., 2014). A researcher analyzing archived data increases the ability to test the validity of the outcome (Berger, 2013). I obtained archived data from the corporations which displayed previous issues and how the breaches were rectified, that information along with the participant interviews provided an excellent data source.

Researchers use ethnography research designs to show how cultures react, social implications, or the communication between groups or individuals (Hoffman & Tarawalley, 2014). An ethnographic design was not appropriate for my study because this study was not observing cultures or how groups reacted to security issues. The ethnographic design is beneficial when attempting to determine cultural characteristics as it relates to gender, race, and class for a study of a group of participants within a certain age range (Lambert, Glacken, & McCarron, 2013). Using an ethnographic approach, the researcher would need to observe the participants for an extended amount of time (Lambert et al., 2013), which is not occurring in my study.

A narrative research design is relevant when the researcher looks to explore the past experiences of their participant (White & Drew, 2011). Loh (2013) also described the narrative research design as discussing participants experiences in detail. The narrative also involves story lines from participants that address sequences of events, cause and effects, and specific activities (Leedy & Ormrod, 2015). The narrative design was not appropriate for this study because the one's life is not the focus of this research. The phenomenological design is a philosophical approach regarding commonalities of people that experienced a phenomenon that was uncommon (Kafle, 2013). A phenomenological approach normally requires a larger participant size than what will be used in this study; therefore, it eliminated me being able to satisfy the sample size requirement. For accurate results the interviewer should have at least 20 participants when using a phenomenological design (Beven, 2014). Robertson and Thompson (2014) viewed a phenomenological study as researching human experience through the eyes of

the people that are living the phenomenon. Since the focus of this research was not to look at the phenomenon of its participants, the phenomenological design was not appropriate for my study.

Population and Sampling

Determining a location and selecting participants for a study should be based off the information that you are trying to obtain and the research that you are attempting to accomplish. I used a qualitative research method and incorporated a census sampling method to select the participants for the study.

Population

The selection of the population should align with the purpose of the study. The population for this study was selected from two medium size businesses that are in the Atlanta, Georgiametropolitan area. The population focused on an estimated population size of seven security managers in those corporations that implemented secure access methods related to cloud computing. Those individuals will have direct knowledge of the security systems that are in place and will be able to provide valuable data for research.,

Sampling Method

The sampling method used for gathering participants for my study wss the census sampling method which is a type of non-probabilistic purposeful sampling method which will allow me to attain data saturation. A census sampling method is beneficial when the entire population can be used or if the population is small (Khosravan, .et al, 2014). My sampling method was beneficial to my study because my sample size was approximately seven participants who met the requirements of being a security manager that ars

employed by the two medium size businesses in the Atlanta metropolitan area that I used selected for my study. A census sampling method can be used when a researcher wants to invite all participants that meet a certain criterion to participate in a study (Jacobson, Hanson, & Zhou, 2015). Utilizing this census method, I was able to obtain information from all the security managers that are present at the business, it allowed for a complete enumeration, which allowed for all participant's experiences to be studied. Using census sampling allows individuals with a high level of expertise and knowledge to be identified and utilized in research to share that knowledge (Pogrund, Darst, & Munro, 2015). Using the census sampling method, I was able to obtain participants based from the requirements as they apply to the study.

If data saturation is not reached there may be a negative impact on research quality which may also relate to validity of data. When I chose the participants that were in the study, it was beneficial to obtain information from all security managers that wereavailable; however, the key with obtaining value information is to obtain data saturation. To reach data saturation there should be enough information obtained to replicate the study, and by interviewing additional participants new data is not attained (Fusch, & Ness, 2015). By interviewing all security managers, I was able to reach saturation at each location. I was able to obtain all information from the participants based on the interview questions. Performing research will not have a set number of participants that are needed, data collection may be completed once saturation is met (Guetterman, 2015; Yin, 2013). My study incorporated all members of the cloud security departments which will allow me to reach data saturation. Performing interviews is one

method that was used to reach data saturation, which was achieved after interviewing the 17th participant (Archambault, Thanh, Blouin, Gagnon, Poitras, Fountain, & Légaré, 2015). To ensure data saturation, follow up interviews occurred, which ensured no new information was obtained.

Ethical Research

It is the researcher's ethical responsibility to explain the purpose of the study, what role the participant's plays, and that their information will be protected Gibson, Benson, & Brand, 2013). Prior to any data being collected, I had to obtain permission from the Institutional Review Board at Walden University. Once I obtained my approval from the IRB, I started the data collection process.. The consenting form was sent via an e-mail to the participants that was selected. The email contained the consent form (Appendix C), which addressed any ethical concerns of the participants, any dangers that may exist, the right to decline or withdraw from the study at any time, and advised that it is voluntary participation. Participants should be advised of how their information will be stored, the length of time, and how it will be disposed of (Kahn, 2014). Prior to the interview, I explained to my participants their information will be stored on a locked usb drive which will be stored in a locked cabinet. Once the doctoral study is completed the information will be kept for five years, and after that timeframe the usb drive will be shredded and burned. The consent form also listed privacy and contact information regarding myself and Walden. The consent form also advised the participants to keep a copy of the form for future reference. By receiving the consent, they were under no obligation to participate in the study. It is important for participants to understand they

can withdraw from a study and not be penalized (Mosse, 2015). The consent form also advised the participants the study was voluntary and they could withdraw from the study at any time. To withdraw from the interview, participants could state such intentions in-person, by telephone, or via e-mail. Robinson (2014) stated researching using financial incentives may result in fictitious information being obtained, Underhill (2014) stated that compensation should not be coercive. There was no type of incentive provided to the participants regarding my study, I didn't want data that was obtained from participants to be influenced by any financial compensation.

When conducting research, it is important to verify that all ethical issues are identified and addressed. Institutional review boards (IRBs), play a major role in determining that research that is being done on human participants addresses ethical issues that relate to the research (Cooper, Borasky, Rosenfeld, & Sugarman, 2016). I did not begin to contact participants prior to IRB approval to ensure that I was following ethical guidelines. Issues regarding ethics have the ability of occurring anytime during research (Khan, 2014). While performing research I did not set false expectation with my participants, make any promises regarding my study, provide or ask for any information that is not related to my study, or ask my participants to provide any information they were uncomfortable providing. It may be regarding the subject matter, data collection, or the data analysis, it is important to have safeguards in place to protect against ethical issues (Buschman, 2014). To safeguard information, all information will be locked and secured, participants personal data was not shared, and participants information was not shared with other participants.

All records (hard copy, electronics, and recordings) regarding the interviews is stored in a safe requiring a combination for access for a minimum of five years. The name of the corporations and the participants names will not be disclosed. Any documentation that has the corporation or the participants names is in a locked safe when not being used. Any documentation or electronic media that Participants information should remain protected for five years for retrieval purposes (Yin,2014). All paper documentation was scanned and stored on a thumb drive and is secured with a password. All additional paper documentation is stored in a locked file cabinet. After that time has passed all hard copy documents and recordings will be shredded, and all electronic media will be erased and shredded. For research to be conducted ethically, the researchers must act in an ethical fashion regarding protecting the participants of the study from a type of harm (Johnson, 2014; Yin, 2014). During this study, ethical guidelines and policies while dealing with participants contained the highest importance.

Data Collection

Instruments

I served as the primary instrument while conducting interviews for my research. When performing research using a case study method, evidence has the capability of coming from six sources: interviews, participant observations, direct observations, archival records, physical artifacts, and documentation (Yin, 2014). Being the primary instrument, I collected data by conducting interviews and information that I obtained from archived data. When performing qualitative research, the researcher will be the most important instrument that will be utilized, this occurs though active listening while

performing direct interviews (Fowler, 2013). Being the primary instrument meant it is important to be unbiased while performing research and conducting interviews. Conducting face-to-face interviews allows the interviewer to visualize body language in response to interview questions (Peredaryenko & Krauss, 2013). During the interview process, I paid attention to the participants for any type of body language or responses that may have led into follow up questions. The lack of face-to-face contact affects the rapport between the interviewer and the interviewee, which may also influence the interviewee understanding the questions that is being asked and needing to ask for additional clarification (Irvine, Drew, & Sainsbury, 2013). For this study, I used open ended questions in semi-structured interviews to collect data.

Conducting face-to-face in-depth interviews allow participants to answer interview questions that have already been created, while at the same time freely discussing additional information that is related (Moustakas, 1994; Yin, 2014). The purpose of using interviews as an instrument was to explore the ideas that security managers have put in place to reach a point of securing information on the cloud infrastructure. Ethical guidelines were put in place during the interview process to keep confidentiality of the participants and to increase validity during the data collection process (Gottlieb et al., 2013; Johnson, 2014). The interview questions (see Appendix A) ensured the ethical guidelines that have been set forth regarding interviewing participants ensured consistency, validity, and trustworthiness of all participants. The interview protocol is within Appendix B, which set the guidelines for the interview process, preceded by the interview questions which are in Appendix A, that have been presented

served as the secondary data collection instrument. Interview questions should be created based off the research question and the type of research being performed (Castillo-Montoya, 2016). The interview questions that were created was based on the research question presented in the study. When I presented those questions to security managers, they were able to directly express issues they have had regarding implementing security processes on the cloud infrastructure.

I also collected archived data from those companies that related to past experiences that occurred with security issues as it related to the cloud to determine what changes were implemented to prevent the issue from reoccurring. Archived data provides a benefit for academic theory due to it being used for comparisons regarding different techniques for research (Opitz & Witzel, 2005). Companies archived data is a recommended secondary data source, Yin (2014) suggests for qualitative case studies. Having the option of collecting archived records is beneficial because participants can provide knowledge regarding company information that may not be public record (Bryde, Broquetas, & Volm, 2013).

To increase the reliability and the validity of the data obtained from participants, I used member checking to revisit the interview results. Richards (2003) labeled member checking as a method of validation, by verifying the data that was gathered from participants for accuracy, based off prior information obtained (p. 287). By using member checking, once the participants were interviewed, follow up interviews were completed to review the information that was received. During this process, confirmation was performed with the participants to ensure information that was gathered was correct

based on their reviewing of the notes and the transcribing of the interview. The member checking process allowed the participants an opportunity to reflect on their words and express additional meanings to those words. It also allowed the participants to advise me as the researcher if any information was transcribed incorrectly during my transfer process (Widodo, 2014). Member checking is effective for establishing trustworthiness due to the information that is obtained from the participants, which are the subject matter experts, it verified several times to validate the information that was received (Loh, 2013). The advantage of using member checking is the ability of understanding the issue from the participants perspective which will add value to the study. The disadvantage of member checking is that it is time consuming because follow up interviews will need to be conducted.

Data Collection Technique

When performing research using a case study method, evidence has the capability of coming from six sources: interviews, participant observations, direct observations, archival records, physical artifacts, and documentation (Yin, 2014). Before any data collection was done I obtained my letter of cooperation from both corporations that I used in my multiple case study and IRB approval. Once permission was granted I worked with the senior security manager at both corporations to obtain the email addresses of the security managers that were used for my research. Once the email addresses were obtained, I sent emails out to my participants requesting permission for interviews. Once permission was granted from the participants, I sent out consent forms (Appendix C) which explained the study and advised them of their ability to withdraw from the study.

Prior to arriving to the site location to perform the interview, reminder emails were be sent to participants regarding the interview, which was a process that was used by Morse and McEvoy (2014), and will be beneficial for me to ensure the participants were available.

I conducted face-to-face semi-structured interviews, which allowed me to focus strictly on the topic which decreased the interviewee's ability to divert away from the topic. A disadvantage of using face-to-face interviews is the possibility of the participants not being available, distortion of results due to biases, or feeling their privacy may not be protected (Bakar, Sulaiman, & Osman, 2014). By contacting the participants prior to the interview and reminding them of the timeframe I was able to ensure they were available, and having one-on-one interviews assisted in protecting the privacy of the participants. It is important to build rapport with interviewees which should reflect in their participation while performing the interview (DiCicco-Bloom and Crabtree 2006, Whiting 2008). One method that I used to build rapport with the participant was to engage in general conversation with them prior to the interview starting. As the interviewees provide more information and it relates to their experiences, it will allow the researcher to dig deeper into the data (Irvine, Drew, & Sainsbury, 2013). Each interview will contain nine open-ended questions which was will related to the participant's experience and issues they had encountered as it related to the cloud.

While performing the interviews the process was recorded to have a record of the participant's response, which afforded me the ability of reviewing the information after the interview. After each interview was completed I reviewed notes that I had taken along

with the recording. This allowed me to address any information that required clarity. Member checking aides in supporting the credibility of data, and the collection techniques (Carter, Bryant-Lukosius, DiCenso, Blythe, & Neville, 2014). Revisiting the recordings, I was able to transcribe the data so that I was able to present that information to the participants for their review. For member checking, members may be asked to review transcripts of their interview to verify the information is correct (Varpio, Ajjawi, Monrouxe, O'brien, & Rees, 2017). I contacted the participants to complete follow up interviews for each participant to review the information that I obtained regarding the interview. This gave the participants the opportunity to address anything that I may have documented incorrectly, and allowed me to ask any additional question to ensure that I reach data saturation.

I worked with the lead security managers to obtain archived data regarding security issues. Having multiple forms of data increases the dependability of the research, which makes data triangulation a valuable research tool (Barnes & Vidgen, 2006). Being able to obtain archived data from both corporations wasthe additional data collection portion to aide in the data triangulation. When trying to obtain past knowledge of “who”, “how”, and “when”, archival data can beneficial in a case study (Yin, 2013). I obtained archived data which views past security practices that were in place and the liabilities and the benefits of them. That information were items that was stored on the server from prior incidents, to physical paper records that were documented to keep track of the issue. Once I received the archived data, I reviewed the data to compare it to the current information which showed security issues in the past and how they were handled. A

disadvantage that could occur would be the data that was obtained during that period of time was limited (Feng, Ling, Neely, & Roberts, 2014). While a limitation of data has the ability of affecting the outcome of data, that is where I used data triangulation in my research which incorporated more than one form of data.

Data Organization Techniques

Being able to organize and store data is an important factor regarding research because it provides a means of being able to locate data more easily and being able to control who may have access to it. Throughout my research I leveraged different systems to organize data that was collected such as reflective journals, research logs, research trackers, and labeling systems (Carter et al., 2014). Each participant's recording was kept separate to avoid data being combined. The recordings were separated by keeping each participant's recording in its own locked folder on an encrypted usb drive. Being able to confidentially code participant's information helps protects their identity and the information they provide (Cseko and Tremaine, 2013). I assigned each participant a special code and keep the coding protected in the excel document, which will be used in place of the participant's names to protect their information. To analyze the data, I used the NVivo software. NVivo can analyze data in a fashion to make the data better understood (Houghton et al., 2013). Having research journals available allows knowledge to be accessible and shared easily (Mahaliyanaarachchi, 2017). I kept detailed journals of my research which allowed for the data to be verified and follow up research to be performed at any time. Ortlipp (2008), used a reflective journal to identify the best framework for their study as it related to the study that was being performed. Utilizing

my reflective journal, I have been able to identify the framework that I felt fit my study and the participants population that would work for the knowledge that I was able to acquire. All data and notes obtained are stored on an encrypted usb drive, and all documents are locked in a file cabinet for five years.

Data Analysis Technique

Gathering, analyzing, preparing, and interpreting data is an important task when performing any type of research, I used a qualitative multiple case study method for my research. I used methodological triangulation regarding the data that was collected to increase validity and reliability. The advantage of use methodological triangulation will be the idea that if there is a flaw in one data source, there would be a strength in another data source to work through the flaw (Joslin & Müller, 2016). Using multiple data sources in my study, I was able to avoid flaws in data that was obtained. The process of analyzing data involves gathering the data, organizing it, disassembling the data, reassembling the information, and determining the relevancy of the data (Mangioni & McKerchar, 2013). Collecting the data and having the information transcribed allows the coding process to occur. The purpose for coding is to identify themes which relate information that is obtained from the participants (Yin, 2014). Marshall and Rossman (2016) also identified coding to identify concepts or themes across interviews

Yin (2014) has identified a five-step process for qualitative analysis: (a) compiling, (b) disassembling, (c) reassembling, (d) interpreting, and (e) concluding. This five-step process was incorporated once data was collected and analysis process was started. Once I completed the interviews, the audio recordings were reviewed along with

the notes that were taken during the interview, that was the compiling process period. The disassembling process was used to analyze the audio and the notes that were taken manually. The data was reassembled and reanalyzed to identify themes. Google Docs and NVivo was utilized for interpretation, which helped to identify themes.

Using the NVivo software I was able to decipher, analyze, and code the recorded interviews. Using NVivo I had the ability of searching through the data by using query and various searching methods. Using NVivo to validate the interview transcripts assisted with identifying themes in the recording, this showed the connection within each recording based off the interview questions. NVivo was the primary tool that was used for the data analysis because it is a versatile application and allows for the information to be exported in Microsoft Office (Edwards-Jones, 2014). Identifying themes from the recordings will help in determining if additional data needs to be collected regarding the study (Marshall & Rossman, 2016).

Coding is beneficial when performing data analysis; however, there may also be disadvantages to the coding of data. Lincoln and Denzin (2011), identified one disadvantage of coding could be that once the researcher decides on the categories to assign data they would be reluctant to look for other categories. To avoid that issue I conducted additional interviews to reach data saturation and identify all possible themes. There are instances when researchers attempt to assign data to certain categories due to not wanting to create a new theme which could pose a problem (Patton, 2015; Yin, 2015). To avoid this occurring, it will be important to remove any biases from the study based on what the researcher wants the outcome to be.

Reliability and Validity

Research may only be considered valuable dependent on the trust the readers have in the researcher's results. The researcher should ensure the data that is obtained is from valid and reliable sources. As a researcher, it is important that the necessary steps are taken to ensure this occurs. The purpose of research is to explore some unknowns and to increase knowledge on certain studies that have been addressed. When conducting research, it is important to perform it without any fabrication, false analysis, deception, or any falsification of data (Christensen et al., 2011).

Reliability

Reliability of data is one of my main focuses during this doctoral study process. Reliability is something that should be considered from the beginning of research. Reliability is affirmation that the approach of the researcher is true and replicable at contrasting points in time (Babbie, 2010). The research process should be consistent based off what is attempting to be studied. This begins with the research question, what type of data is being collected, how data will be collected, and the methods of how the data will be analyzed. Svensson and Doumas (2013) suggest one method of ensuring reliability in research is to ensure the research method stays consistent throughout the study. Ensuring that research information is documented properly ensures repeatability of that data that is being collected (Turgut, 2014). When utilizing case study research, reliability can be shown if another researcher using the same procedures obtain similar results (Yin, 2014). Reliability was established by ensuring consistency of the processes used during the interviews that was outlined.

Dependability

The trustworthiness of data that is collected and analyzed is the foundation of high quality qualitative research. The data that is obtained should be similar for the participant, and be detailed. Researchers must stay neutral while evaluating data, which incorporates sampling and data analysis, for the study to be dependable (Daigneault & Jacob, 2013). Member checking incorporated in a study increases dependability and creditability. Using member checking allows participants to verify the information that was obtained which validates the credibility of the data (Richards, 2003). Utilizing member checking a researcher will be able to validate that data saturation is met through no additional themes, coding, or information will appear (Ajagbe et al., 2015; Birt et al., 2016; Marshall & Rossman, 2016). The processes for collecting the data was documented, which included interview protocols, recordings, and all notes that were taken.

Validity

When using the case study method, the researcher will use data triangulation to present the same conclusion which will increase the validity of the study (Leedy & Ormrod, 2010). Qualitative researchers look to identify methodological strategies to ensure the trustworthiness of findings. Trustworthiness corresponds to validity, when data is obtained from trusted sources, which increase the validity of research. By utilizing member checks as a part of response validation, this will eliminate inaccuracies between what the interviewee says their qualifications are and how they respond during the interview process. Member checking may also occur toward the ending of the research by

having the participants review your interpretation of the information that was gathered, which will increase validity of the data (Andraski, Chandler, Powell, Humes, & Wakefield, 2014). Validity was further addressed by obtaining data from multiple sources, which was done by looking at archived data from the company's and one-on-one interviews.

Credibility

In qualitative research credibility refers to a correct portrayal of information through interpretation or description of the participant's experiences (Tong, Chapman, Israni, Gordon, & Craig, 2013). Using member checking allows participants to verify the information that was obtained which validates the credibility of the data (Richards, 2003). Member checking allows participants to read a summary of the recorded interview that was transcribed to verify its accuracy, which enhances its credibility (Houghton et al., 2013). During the interview process the information obtained was recorded which allowed for the information to be reviewed later. The same interview questions were used to ensure the same protocol was enforced with all participants, which also maintained credibility and avoided skewing of the data that was obtained.

Transferability

Transferability is described as the extent in which the research can be transferred to other contexts (Venkatesh et al., 2013). Utilizing purposeful sampling a researcher is able to enhance transferability (Liu, Tang, Wang, & Lee, 2013). Elo et al. (2014) characterized transferability as the capability of being able to utilize the findings from one research and use them in another type of research. Transferability will be established

by keeping detailed and accurate records of the data that was obtained from the participants, and by verifying the data that was collected was from credible peer reviewed sources. All information will have the ability of being verified which enables other researchers to use the data.

Confirmability

To establish confirmability, participants reviewed transcripts of the face to face interviews that was performed, which allowed them to ensure the information that was transcribed was correct. Confirmability was also accomplished by consistently verifying the data that had been collected throughout the study. Confirmability occurs by establishing and managing a chain of evidence that coordinates data collection and data analysis to the conclusion, showing the research to be credible based of the viewpoint of the participants, validation methods, and the sources utilized to collect the data (Andrade, 2009). Confirmability is a detailed means to certify goals that are outlined in a qualitative research study (Houghton et al., 2013). Being able to provide information that has the ability of being confirmed adds validity to data that is collected.

Transition and Summary

This study will address the issues that some cloud security managers lack strategies to implement secure access methods to protect data on the cloud infrastructure. Section 1 covered the research problem, purpose of research, nature of study, interview questions. The framework that will be utilized and the literature review. The literature within Section 1 encompassed data regarding studies related to access vulnerabilities while utilizing the cloud infrastructure, issues that have occurred due to inappropriate

security methods, and various studies that have utilized the technology acceptance model to validate the acceptance of the cloud technology. Section 2 will contain in depth information readdressing the purpose statement, and regarding the role of researcher, details about the participants, research methods and design, population and sampling, data collection (instruments, techniques, and organization), data analysis, and the data reliability and validation techniques.

Section 3 will include the overview of the study, findings of the study, implications for social change, recommendations for actions and further studies. Section 3 will also encompass the reflections of the study in which I discussed my experience throughout the research process. Section 3 will close out the research with a summary and the study's conclusion.

Section 3: Application to Professional Practice and Implications for Change

The focus of this study was exploring strategies used by cloud security managers to implement secure access methods to protect data on the cloud infrastructure. In this section, I explore the use of the presented findings from individuals that are in the profession. The section also includes a (a) presentation of the results, (b) application to professional practice, (c) the implications for social change, (d) recommendations for action, (e) recommendations for further research, (f) reflections on my research experience and the study conclusion.

Overview of Study

The purpose of exploring this topic was to show the importance of protecting information that is stored on the cloud infrastructure. Based on information that was obtained throughout this study, my aspiration is to show the ability that some organizations have regarding protecting assets and private information that is stored on the cloud infrastructure. Based on information obtained from participants, the pain-points that affect security relates to lax authorization methods, which relates to the end-user and the company that is placing regulations on those methods.

While keeping security simple based on authentication methods may be beneficial in some instances, there are certain security options that must be implemented to remove vulnerabilities (Kreutz, Esteves-Verissimo, Magalhaes, & Ramos, 2017). Having an understanding that authentication is one of the first steps that allows users access to certain portions of the cloud infrastructure. Granting users access based on their roles

provides access to only what is needed, which sets the initial security point (Rizvi & Fong, 2016). One of the biggest threats to a cloud network would be an internal threat if the rights are not granted properly, users have access based on roles, and having roles which gives full access to a network gives a hacker all the tools they need. Being able to manage authentication and access control over the cloud is a major challenge that cloud providers address (Naik, & Jenkins, 2016). Having strong authorization and authentication policies in place will safeguard information that is stored on the cloud infrastructure.

Presentation of the Findings

The research question used to explore the study was as follows: What strategies are used by cloud security managers to implement secure access methods to protect data on the cloud infrastructure? For coding of information that was gathered from participants and archived data, I used NVivo 11, which helped identify the frequency of key themes. There were three primary themes that surfaced from the analysis of archived data and the transcribed data obtained from the participants through interview questions. Those themes were; (a) Implementing Security policies, (b) Strong authentication methods implemented, and (c) Strong access control methods implemented. For this multiple case study, I used the TAM as the conceptual framework for what strategies cloud security managers use to implement secure access methods to protect data on the cloud infrastructure. The TAM framework can examine a person's will to use a security method based on its (PU) or the (PEU) of the application (Davis, 1989). I examined the

interview transcripts and the archived data obtained from the participants, to determine if the (PEOU) or (PU) was present.

Security policies implemented

Implementation of security policies was one of the themes that arose from the interviews. Security policies being properly addressed and followed was a key item that was discussed involving protecting the network. It is important that security managers verifying security policies address the requirements for the organization to follow, which may be basic as a password that is chosen to what you may connect to on the network and be able to access. Security managers implement security policies to address how corporate and guest networks for individuals are handled and what may occur during its usage. When security policies are created, the primary goal is to protect assets from any threats, the next consideration is cost, and the final consideration will be the user (Chou, 2013). Understanding how and when to create an optimal security policy will result in benefits for the company and the user.

Implementing security policies was a theme that all seven participants discussed and noted was important. Seventeen of the 21 archived organizational documents addressed the theme (see Table 2 for source metrics). All seven participants indicated that implementing a solid security policy is important to protect resources. They also stated that when a security policy is lacking support, individuals are not likely to enforce it, which creates vulnerabilities within the network. Twelve of the 21 organizational documents addressed ensuring the enforcement of a solid security policy and that having

weak policies in the past created issues regarding the cloud infrastructure being infiltrated which resulted in additional cost to resolve those issues.

When discussing benefits, ease of use, and convenience, there was a discussion regarding users understanding the purpose of implementing a new security policy. This discussion introduced the benefits regarding users' acceptance of the security policy, six of the seven participants felt that users didn't see a benefit of using the new policy over what was currently in place, so they chose not to use it. Seventeen of the 21 corporate documents spoke on users benefits of accepting a new policy and how the changes in the policy provide protection of its resources.

Table 2

Table 2. *Major Themes of Implementing Security policies with Supporting Metrics Minor Themes of benefits of security policy with Supporting Metrics*

	Participant		Document	
Major/Minor Themes	Count	References	Count	References
Implementing a security Policy	7	48	17	56
User's benefits for acceptance of the policy	6	20	15	37
Stakeholders benefits for acceptance of the policy	7	32	13	31

All seven participants discussed the benefits for stakeholders regarding the acceptance of the security policy being implemented. As a security manager, it's important to get the acceptance of the stakeholders regarding the security policies and to show they bring value to the corporation. One participant stated that when attempting to bring the stakeholders on board to accepting the need policy we needed to show why the

change was needed, and if the price of the change matched the benefit. The statement from some of the stakeholders was, if the current policy that's in place is working, why do we need to change it, and from the standpoint of the security managers, there is never an option to keep things standardized regarding protecting data.

Thirteen of the 21 organization documents that addressed the needed support from the stakeholders regarding the adoption of the new security policy to stay ahead of attacks. The information obtained from the documents expressed the lack of support created delays in prior policies which affected the policies being fully implemented.

Having an understanding of why implementing the security policy being accepted aligns with the selected conceptual framework. The PEU has a positive effect on the usefulness and the adoption of technology (Schoonenboom, 2014). One of the participants noted that one of the factors for the security policy that was implemented was its "ease of use and convenience." Policy changes occur to intercede on new threats; by addressing these issues, and having users accept the change, companies are less likely to incur breaches. McIntosh (2017) used the TAM to explore why changes within strategies and polices were made to implement mobility products relating to the cloud. The conclusions of the study were the (SREB) only strategy was to keep of with the needs of their customers, not to focus on implementing security on the cloud. While exploring how the TAM was used regarding the adoption of computerized system Rogers (2016), looked at policies and procedures to determine what was currently be used, and how those policies may affect adoption.

Researchers explored methods regarding using the TAM was used to show the (PEU) and the (PU) with implementing a new technology. Okundaye (2016) used the TAM to explore how the PEU and behaviors related to the implementation of new policies and the adoption of ICT. Having clear information security policies in place influences users attitudes regarding their informatin being protected (Lu et al., 2013). One participant noted that one of the factors for the security policy change was based on current industry standards and the old standard was useless. The participant also stated the new policy has the ability to provide security in layers which enables more control when changing policies. Osho and Onoja (2015) stated it is important to implement a standardized security policy to aide in securing cyberspace. One participant stated, "the key to implementing a strong security policy is to show how not having a strong security policy cost more money."

Reseachers have performed studies using the conceptual framework to explore how users benefit from the acceptance of policies. When policy changes occur, professional research is done to ensure the change is beneficial and may help with technical advancement (Mao-Yu, Li, Hu, & Yi-Tao, 2015). When addressing the user's benefits of a new security policy, "the functionality of the equipment and the adaptability of the user were factors when creating the new policies", as stated by a participant. While addressing change and protection of a new system, policies and regulations should be the first step when ensuring the normal functionality of equipment (Peterlongo, Ionescu, & Gavrila, 2015). Users may not see the benefit of a policy when they do not understand the reason for a policy change. A new security system will only prove beneficial to users if

the policy is implemented and understood by all parties involved (Al-Mukahal & Alshare,2015).

One participant stated that, when a user understands a benefit in a technology, they are more likely to use the technology. One participant stated, “we do not give users an option not to use the technology that is being implemented, because we have individuals that access the cloud from various locations, we must ensure their devices and what they access is secure.” Even though security is the main goal, participants must see the benefit of their information being secure based on this change.

In a study conducted by Ramírez-Correa, Arenas-Gaitán, and Rondán-Cataluña (2015), they used the TAM to evaluate if users that were at different locations, where the universities used cloud technology, adopted the e-learning technology. The researchers examined the relationship between PEU perceived ease of use and external controls to determine the adoption of the e-learning technology. User have stated, “that in the past, when there have been changes, there have been learning curves that create a longer timeframe to complete tasks which create a dislike of the technology, a participant noted.” When users find technology less complicated to use they will have a positive outlook for its usefulness (Iqbal & Bhatti, 2015).

When trying to implement a new technology, the first group that needs to be on board will be the stake-holders, because they affect the budget. Ray (2016) used the TAM to view the stakeholder analysis to view their benefit regarding the acceptance of the adoption of the cloud. With any changes, stakeholders view the negative issues first prior to understanding the benefit that arises from a change. Van Dijk, Fischer, Marvin, and

van Trijp (2017) performed a study to examine the perception on the attitudes regarding stakeholders adopting the nanotechnology based on the risks and benefits. Based on the findings in the study the authors felt the need to explore the subject further when trying to compare the acceptance to the new technology from the stake-holders in relation to the acceptance of the technology from the public (van Dijk et al., 2017).

The data that I collected from the interviews and the archived data showed the benefits of the stakeholders adopting the new technology. Cabral (2016), used the TAM to explore if perceived ease of use and perceived useful were factors regarding the selection of projects, relating to what the stake-holders may seem feasible to utilize resources on. One participant noted, if the stake-holders do not see a benefit the department will not receive the funding.

McIntosh (2017) used the TAM to explore why (SREB) owners use certain strategies to implement cloud and mobility products to reduce technology cost. The stakeholders view benefits based on the savings they see from implementing a new technology, and how effective that policy may be. The organization data show how stakeholders were on board with new technology and saw the benefits after information was presented that showed a savings in time and money. Balavivekanandhan and Arulchelvan (2015) showed that ,for stakeholders to be on board with a new technology, the intent to use would first have to be established.

Strong authentication methods implemented

Strong authentication methods being implemented was the second theme that arose during data analysis. Authentication methods provide various means to verify that a

person has access to network resources. Authentication is the process by which a person that is trying to gain access to a secure domain is being verified by using correct credentials; in the event the incorrect credentials are used the person will not have access to that secure domain. The authentication items will normally consist of a username and a password to gain access. Based on the authentication methods that are established by the security managers and by policies, will determine the items required and how many times a user must authenticate.

Strong authentication methods was an item that each participant discussed. Fifteen of the 21 organizational documents addressed the theme (see Table 3 for source materials). All participants indicated that having strong authentication methods in place increases security. Participants stated that the key to having strong authentication is being able to confirm who is trying to gain access to the network (through username and password), and one of the methods for achieving that is network access authentication which grants access to all network resources based on rights. “By the users authenticating properly and gaining access to the network, their device will be checked to verify all security is updated prior to granting full access which protects the network”, noted a participant. This prevents the user from having to re-enter their credentials each time, which is time consuming and may cause the issue of the user creating a shorter password just to save time.

Multifactor authentication was addressed by five of the seven participants which stated, multi-factor authentication was chosen because it was the right thing to do at the time. Utilizing this method not only requires a password but also an additional method

for the user to verify who they are. “The second factor of authentication varies based on the department that you are in and what you have rights to” stated one participant. From the security department, “we have certain access which enables us to see all accounts and what users are doing, if a person has obtained our credentials this could have a large impact on the network,” as said by a participant. To access the network, the second form of authentication is fingering printing scans, and when PC’s are used off the network the VPN must be used to gain access to the network. The participants also stated, when access is provided to standard users they will use their user ID and their password, which must meet the assigned standards. Multi-factor authentication has provided an extra form of protection by having users think of another method they can use to authenticate with.

When addressing multi-factor authentication, 13 of the 21 organization documents addressed multi-factor authentication, which uses friction to increase security on the network by monitoring how a user gains access to the network, what type of device they use, the browser they use, and looking at the operating system. When we speak on friction, the methods that are referred to are noticing when there is abnormal activity occurring on a person’s account. If the user logs in and their device is showing a different screen resolution, outdated software, browsers and possibly no security, and records show the user has updated all of this, there is a problem, and someone has gained access to that person’s credentials. Some individuals see friction as an inconvenience, and it can be in some forms; however, it’s an additional form of security, noted a participant.

Table 3

Table 3. *Major Themes of Authentication Methods Implemented with Supporting Metrics*

Minor Themes of Multi-Factor Authentication with Supporting Metrics

Major/Minor Themes	Participant		Document	
	Count	References	Count	References
Strong Authentication Methods Implemented	7	42	15	63
Multi-Factor Authentication	5	30	13	51

The reason why a Strong authentication method was chosen aligns with the TAM framework because the user and the business needs are determinants in its adoption. Svilar and Zupancic (2016) used the TAM to analyze how users perceive security and how the authentication methods that are in use affect the perceived usefulness. The ability of a user being able to utilize the method has an impact on how effective the method will be. Improper authentication influences perceived risk, which affects a user's perception of usefulness regarding the access being secure (Mohammadi, 2015). Utilizing the TAM framework (Mohammadi, 2015), explored the perceived risk as it applies to the resistance regarding the implementation of a certain authentication method. "Prior to authentication methods being enforced, risk assessments were performed and surveys were given to the stakeholders" as mentioned by one participant.

There is literature that has been created that discuss the reasons for the need of a strong authentication method. Chandrasekaran (2015) discussed using a single sign on authentication option to access multiple systems as a means of authentication. The authentication step for the cloud network is important because without the correct credentials the person will not have access to the network, as mentioned by one user. Ghazizadeh et al., (2014) used a single sign-on authentication method that was introduced

to combat security issues on the cloud. The primary method of protecting resources is to control what may be accessed, a person can't get into a building if the door is locked and they don't have a key, an example used by one participant. Ghazizadeh et al., (2014) used a single sign on method for authentication that was introduced to combat security issues on the cloud.

The collected data supported the TAM by users choosing multiple-factor authentication based on its perceived usefulness. Multi-factor authentication is easily accepted when users can personalize the information they use to authenticate, as indicated in the documentation obtained. Park and Kim (2014) incorporated the TAM to investigate user's perception on adopting mobile cloud computing when users could user personal authentication options (Nikou & Economides, 2017). When discussing security, users may not understand the importance of authenticating or the importance of keeping that information private. How a person perceives security has an impact if they will take the necessary steps to keep information protected. A study conducted by Shah, Peikari, and Yasin (2014), suggested that websites that asked for users to authenticate to make purchases created a perception of trust from the user, the customer's perception would be positive regarding using that technology. Users are less-likely to use strong complicated passwords because they are more difficult to remember, they will migrate to things they always remember, which is why paraphrasing was a method that was implemented on our network, stated a participant. Even with implementing multi-factor authentication, passwords are still the most common form of authentication, to deal with the increased complexity of passwords, paraphrasing can be implemented, which allows a user to

incorporation something common to them while still having security (Keith, Shao, & Steinbart, 2009).

Authors in the literature have discussed the benefits of having additional forms of authentication to increase security. When users have multiple items that may be used to gain access, it decreases the chance of a network breach. Khamlichi and Chaoui (2016) proposed adding an extra level of authentication on the cloud, which is an additional form of security. There have been test on the network regarding images as an additional form of access, while we chose not to use images as an additional form of access, we have used them to ensure the person that is attempting to access the network is not a bot. Abdellaoui et al., (2016) used a form of authentication that incorporated images by installing an AuthMode application which validates the image that the user chose.

Strong access control methods implemented

Strong access control methods being implemented was another prominent theme. The access control methods were described by security managers as methods that are used to gain entry to the cloud infrastructure. Access control methods play a critical role regarding access to a network and protecting information that is stored within that network. Access controls have two categories, which are physical and logical, physical relates to access to actual organizations, where the logical relates to technology (computers, networks, servers, etc.). The job of the access control is to first authenticate whomever is attempting to gain access, and once that person has been authenticated, through using a correct username and password they may be granted access to those resources in which they are entitled.

All seven participants indicated that access control methods are a main contributor for denying unauthorized access to resources, and those methods was mentioned in 20 of the 21 organizational documents (see Table 4 for source materials). People don't understand that just denying access to a physical location to people that should not be present is a major step regarding security as noted by one participant. Access control starts from the basics, and then enters the technology world one participant stated. Controlling whom has access to the cloud means we are controlling who has access to private information, if there were no checks and balances anyone could have rights to all information, which affects the credibility of this corporation. One of the key methods for controlling access is through an access control list, which grants access to individuals based on rights, as explained by participants. Being able to restrict access based on the ACL's decreases threats that have occurred. Four of the participants stated that the more stringent the security is regarding access, the less time we must focus on cleaning up issues after a breach.

The benefits of having strong access methods was discussed by six of the seven participants and in 15 of the 21 organization documents. One of the benefits that participant one spoke on is regarding the software access method that is used, because the functionality of the application is easier and it provides less of a headache for the end user, the application allows for controls to be set and based on the rights that are assigned to the user, that will determine what that user can or cannot access. Another participant spoke on the benefits of the logs being kept whenever a user attempts to log in or logout, having a log gives an indication if there is abnormal use and the issue can be addresses

quickly. By using an Identity Management System, the process is automated, which decreases room for error, and removes the manual process for assigning users control. Organization documents comment on past processes where the process was manual for assigning rights to users and over time there was not an accurate account of what the user should have, which created network vulnerabilities.

Table 4

Table 4. *Major Themes of Access Methods Implemented with Supporting Metrics*

Minor Themes of Role-Based Access Implemented with Supporting Metrics

Major/Minor Themes	Participant		Document	
	Count	References	Count	References
Strong Access Methods Implemented	7	42	15	63
Benefits of Strong Access Methods	6	36	15	57

Access methods being implemented aligns with the conceptual framework because the choice of adoption aligns with its perceived usefulness. Hsu, Lee, and Su (2013) used the TAM to see how access control methods are designed to increase security to protect the Healthcare Information System, which is used to ensure that only authorized users have access to the health records. One participant stated one of the main goals for access methods is to mitigate risks, “while we may not be able to stop all things, we are able to place some control on how bad it may become”. Having heightened access controls methods limits who may have access to system resources that contain private information (Hsu et al., 2013). If a user does not see the purpose of an access method

they may try to avoid using it, or attempt another means of accessing resources, some users may attempt to locate a backdoor if they feel that saves time working on an issue, noted one participant. Access methods will only be beneficial if they are chosen and used, and users must decide if the method is convenient, even if they find it to be useful (Mathieson, 1991). While we don't give users choices regarding the security portion of access methods, the means in which they access a resource may be up to the user. Research has shown that access methods can be used to monitor how consumers access certain website and the reason why they choose to return to those websites monitored by the technology acceptance model, users having a perceived usefulness has great value on them accessing that website another time (Koufaris, 2002).

In literature, Chou (2013) discussed setting controls in access methods which allows security managers to filter content, and deny unauthorized access. Information obtained from organizational records showed access methods have been used which block users from content that is not job related, it provides a means of users being able to have read/write access to only what is needed. If users fail to use the proper access methods, they will not have access to the network resources, because they would not fully be on the network. In literature obtained regarding access controls and users behavioral intent to use access controls based on the security requirements that are set forth by the corporation, if a user is not given an option to dismiss the access method are they forced to comply (Johnson, 2013). As discussed by Sen (2013), with the cloud being accessible to anyone on the internet, proper access methods are more important than ever.

Understanding the benefits of strong access methods aligns with the conceptual framework relating the perceived usefulness to access methods providing a valuable service. One of the benefits of access controls in a study conducted by Al-Maliki (2013) using the TAM showed perceived ease of use and perceived usefulness for methods that denied access to users that may be suspected of inappropriate usage. One participant highlighted the fact that having the automated user creation in place has saved time and made expansion a lot easier. Having cloud access controls provide flexibility regarding growth because it provides the ability of integrating users by using the access control list (Goh et al., 2003; Bethencourt et al., 2007). Based on information that's stated in organizational data, implementing identity and access management allows credentials to be assigned easier, which also allows manage of resources to be more controlled. Authors have performed studies showing the benefits of strong access methods being able to manage access to recourses, based on the user's credentials being verified, this increases security regarding network access (Sharma, Dhote, & Potey, 2016).

Literature has shown that with a successful access-control method created users perceive there is more of a privacy benefit than just using a password (Chi-Lun, 2014). While access is granted to a user once their username and password is verified, what they may have access is based on their limitations of access. One participant voiced they were happy to see a decline in outdated user accounts with the implementation of the new identity management system which allowed them to clear out accounts for people that were no longer employed. With access control being policy driven, it produced different arenas for other identity management systems to be implemented, which helped reduce

risk and increase security (Stoetzer, 2016). By having access controls in place, it provides more protection for internal and external users, a main benefit of access control is automation. One of the concerns when users decide to adopt the cloud is related to protections and access controls, if those controls are not setup properly (Sharma et al., 2016).

Applications to Professional Practice

The professional IT impact is the findings from this study may benefit cloud security practices by informing technology specialist of practices that are currently utilized to secure information. Participants that provided information for this research supplied information based on strategies that are used in their corporations to keep their cloud infrastructure secured. Many cloud service customers may not have the knowledge to perform risk assessments regarding the cloud or do not employ people with the IT expertise to understand the technology to make a decision regarding its functionality (Cayirci, Garaga, Oliveira, & Roudier, 2016). While the goal of both companies was to provide security to the network, there was some variation regarding how that goal was reached. Each company's initial security methods have evolved to protect the internal information regarding the corporation and the external information that applies to the consumer. The data collected from the participants tailored to which practices worked best for the corporations while still protecting data. After the data was evaluated, there were three themes that were identified: Security policies implemented, Authentication methods implemented, Access methods implemented. The results that were obtained

from this data can be used as a foundation for organizations to check their current security methods.

Corporations that utilize the cloud for the networking and storage services can use the results from this study to make updates to their current processes and policies. The changes to the process can address automation regarding processes, this would remove the human error. Role management programs that automatically creates users, provides an automated process for controlling users access and activities (Peñaloza-Salazar C., Gutiérrez-Maldonado J., Ferrer-García M., et al., 2015). The policy may also recommend that risk analysis be performed periodically to ensure the updated process is still functioning properly. A corporation where their goal is to secure the privacy of the company and the consumer can follow guidelines based on data collected from participants. Polices should be created and set throughout the corporation so there would be consistency company wide. Da Veiga (2016) performed a study regarding individuals that read the policy and users that did not, the study showed that individuals that read the security policy has a positive outlook on the security policy and was prone to follow its guidelines. With any change that occur, communication must occur, and responsibilities must be stated to all parties that are involved. If implemented properly, corporations should benefit from data that was gathered from this study.

Implications for Social Change

The initial social change for this study was to decrease the customers concern regarding information that is stored on the cloud being compromised. The combination of consumers feeling confident in using a product, understanding a need for the product, and

understanding their privacy is being protected increases acceptance of the cloud infrastructure (Ratten, 2015). Many consumers do not understand how the cloud works or the process that's involved with how they access information. By showing users that information can be safe while being stored at an offsite location should reflect a positive change. A positive change in a customer's mindset may decrease user's fear of their private data being compromised, and build trust between the consumer and the corporation, which may increase cloud utilization. Having an idea of what the customer's needs are, how they will use the cloud, and what fears they have regarding the cloud are factors that relate to consumers adoption of the cloud (Habjan & Pucihar, 2017). While my initial social change still applies regarding the customers concern, my implication for social change has expanded to corporations also.

The study was explored looking at two of the constructs which are: perceived ease of use and perceived usefulness, which are factors regarding why certain security methods were incorporated. The results of the study showed that PU and PEOU influence why users adopt certain security methods and why users elected to use certain security platforms. The TAM is one of the most commonly used frameworks for understanding the adoption of a technology, due to its focus on perceived ease of use and perceived usefulness (Davis *et al.*, 1989). PU seems to be dominant when users elect to adopt the technology because they don't want to waste time. The results of the study show that PU and PEOU have the ability of predicting if a user will adopt a technology.

Study results show two corporations that have benefited from the current security methods they have in place by having a secure infrastructure. Corporations making

changes to security policies based on knowledge that is received from the study can have a direct effect on how information is accessed and secured. The collected data may also relate to how users are educated on enforcing of the policies and procedures. The findings in this study may also offer strategies that may be used to address current security concerns internally, regarding employees, and externally look at all threats.

Recommendations for Action

The purpose of this qualitative case study was to explore strategies used by cloud security managers to implement secure access methods to protect data on the cloud infrastructure. Based on information that was obtained from security managers during this study there were three items that were addressed when exploring information related to protecting information that is stored on the cloud infrastructure. The first recommendation is that corporations have a standard security policy that is in place and ensure that it is being implemented. IT teams having a set IT policy in place for cloud usage sets standards for users to follow (Attaran, 2017). The security policy should be detailed and should be understood by each employee. The employees should be educated on the reason for the policy and sign the security policy to show their understanding of the policy and understand there will be repercussions if the policy is not followed. The participants that were interviewed for this study have a solid security policy that was in place and enforced.

The second recommendation is for corporations to do risk assessments on their current authentication methods, which tests their effectiveness. Anytime there is an instance of data moving to and from the cloud, there should be an impact assessment

performed (Cayirci et al, 2016). If the corporation is not currently utilizing effective access methods, they would need to take the necessary steps to invest in either having third party companies to come in and offer their services to see which would be best for the corporation, or have their internal IT department address the weak authentication methods. If the current authentication methods that are in place only look for one form of authentication, that would need to be addressed to increase security. This current method was effective for both corporations that were in the study.

The third recommendation is regarding the access methods that are used to access the cloud. Users have an expectation of faster and easier access to relevant information for heightened operational efficiency (Shiferaw & Cerna, 2016). The security regarding the access methods need to be addressed, whether the methods are software access where the services are accessed remotely, or if the data is being accessed onsite. The software method gives the corporation the ability for faster expansion in the event of company growth. While the software method of access provides less overhead to the corporation, the user that's accessing the data needs to be mindful of keeping they credentials protected. Educating users on the importance of how information is accessed, and securing that information will be useful. This information can be provided to various corporations that support and want to provide secure access to the cloud infrastructure.

Recommendations for Further Study

The findings for this study provide a basis for further research in the areas of security regarding the cloud infrastructure. This qualitative multiple-case study focus on two corporations that are in the Atlanta Metropolitan area, which raised two limitations.

The first limitation referred to participants may respond to interview questions based on what they believe the interviewer wants to hear, and the second is that data collection was limited to two medium sized businesses in the Atlanta, GA metropolitan area. The participants in this study provided valuable information based on their experience, knowledge, and time at the corporation. The participants shared information regarding current processes and detailed information on why those processes and policies are in place. Researchers have the ability of expanding on this research by broadening the participants outside of the cloud security personnel. The researcher can look at the issues from the user's standpoint regarding security issues they experience. The study focused on two medium sized businesses in the Atlanta, Georgia metropolitan area. Recommendations for further research would be to expand to other geographical areas, and use larger corporations. Additional research can be performed utilizing a quantitative method in which the researcher can examine a larger pool of participants and examine financial loss as it applies to security vulnerabilities when not addressed compared to the cost of implementing a secure system.

Reflections

When I initially began this degree track at Walden University for my Doctorate in Information Technology I didn't know what to expect. I began the program and realized there would be some long days and nights, and not many free weekends. Preconceived notions that I had were due to hearing horror stories from other individuals that have attempted to obtain a doctorate degree and their inability to complete their course workout, or the dissertation. I felt I was prepared for the program, I did a lot of research

while working on my Master's degree and felt that my writing improved from my undergrad writing style. The research courses that were in my D.I.T. program provided a strong foundation for preparing me to begin my study. Two courses that really stood out to me were the quantitative and qualitative courses. During both courses, I had the ability to research both methods to understand how each was used. Prior to both courses I had never looked at a study from a qualitative or quantitative standpoint.

I chose to research cloud security, because security has always been an interesting topic to me. With the increased usage of the cloud and the increased threats that have occurred I believed this would be an interesting topic. Most people use the cloud daily and never realize how it functions or that information they are storing and accessing is handle by a third party. I have worked in information technology for over 15 years, however, I have mostly been on the hardware side and not addressed a large amount of security issues. I felt this would be a good transition to explore the other side of information technology while gaining knowledge regarding its functionality.

The participants in this qualitative multiple-case study provided knowledge regarding methods they use to keep their cloud infrastructure secured. I felt that having interviews discussing the positive aspect of their network created a smoother interview. They were eager to share their policies and processes, they were also willing to speak on what did not work in the past. I gained valuable information on how the companies chose security policies and that even a cheaper product, while may work currently, was not beneficial when looking at expansion. One statement that I received from a participant that I will always remember is "we spent more money making a free product work, than

we would have if we had just paid for a product". I had no relationship with any of the participants prior to the interviews which assisted me in avoiding biases. The interview questions were open ended questions which did not sway the interviewee to any type of response to avoid any additional biases.

Summary and Study Conclusions

The ability of securing a network to protect data can be a challenging task. In aspiring to show the possibility of data being secured on a cloud infrastructure, I hoped to bridge gaps in knowledge relating to the cloud. Users may always have doubt when having their personal information being stored on the cloud; however, proving that data can be accessed safely provides comfort to end users. To secure a network it takes a combination of risk assessments, experience, knowledge, resources, and policies in place to mitigate those issues. There is not a one-size fits all when it comes to securing information, it will depend upon the need of the individual or the corporation. The findings in this study showed the ability of two corporations understanding there are security issues that occur on the cloud infrastructure and those issues needed to be addressed. Those corporations have the ability of having secure access methods, which protects user's identity and their resources. Stakeholders and security managers must understand the goal of security and work together to create standards and to put those standards into action. They must also utilize strategies that will be effective and compliment the business need. Learning from prior experiences allows security managers to thwart future issues. The overall goal for securing a network is to protect the internal and external resources, while increasing the trust with the user.

References

Abdellaoui, A., Khamlichi, Y. I., & Chaoui, H. (2016). A BYOD method for enhancing authentication in the cloud environment using elliptic curves. *International Journal of Computer Science and Information Security, 14*, 63-68.

Adjei, J. K. (2015). Explaining the role of trust in cloud computing services. *Info: The Journal of Policy, Regulation and Strategy for Telecommunications, Information and Media, 17*, 54-67. doi:10.1108/info-09-2014-0042

Ahmadipour, H., & Hajmohammadi, F. (2016). Horizontal integration in basic sciences at kerman university of medical sciences: Medical students' viewpoint. *Research and Development in Medical Education,* 5, 93-96. doi:10.15171/rdme.2016.019

Ajagbe, A. M., Sholanke, A. B., Isiavwe, D. T., & Oke, A. O. (2015). Qualitative Inquiry for social sciences.

Akintomide, O. A. (2013). Cloud computing: the third revolution in it. *Library Progress International*, 33(1), 77-95.

Akpabio, A. E. E. (2013). Chief information officer's role in adopting an interoperable electronic health record system for medical data exchange (Order No. 3569908).

Al-Bakri, A., & Katsioloudes, M. I. (2015). The factors affecting e-commerce adoption by jordanian SMEs. *Management Research Review*, 38, 726-749. doi:10.1108/mrr-12-2013-0291

Al-Maliki, S. (2013). A new plan for king khalid university (KKU) central library to revitalise academic E-resource-sharing. International Research : Journal of Library and Information Science, 3(4)

Al-Mukahal, H., & Alshare, K. (2015). An examination of factors that influence the number of information security policy violations in qatari organizations.*Information and Computer Security, 23*(1), 102-118. doi:10.1108/ics-03-2014-0018

Ali, M. & Cullinane, J. (2014). A study to evaluate the effectiveness of simulation based decision support system in ERP implementation in SMEs. *Procedia Technology, 16*, 542-552. doi:10.1016/j.protcy.2014.2014.10.002

Allam, S., Flowerday, S. V., & Flowerday, E. (2014). Smartphone information security awareness: A victim of operational pressures. Computers & Security, 42, 56-65. doi:10.1016/j.cose.2014.01.005

Aleem, A., & Ryan Sprott, C. (2012). Let me in the cloud: analysis of the benefit and risk assessment of cloud platform. Journal of Financial Crime, 20, 6–24. doi:10.1108/13590791311287337

Aleem, A., Wakefield, A., & Button, M. (2013). Addressing the weakest link: Implementing converged security. *Security Journal, 26*, 236-248. doi:10.1057/sj.2013.14

Aldwairi, M., Masri, R., Hassan, H., & ElBarachi, M. (2016). A novel multi-stage authentication system for mobile applications. *International Journal of Computer Science and Information Security, 14*, 389-396.

Al-Rashedi, A. (2014). E-government based on cloud computing and service-oriented architecture. *International Journal of Computer and Electrical Engineering,* 6, 201-206. doi:10.7763/IJCEE.2014.V6.822

Alseadoon, I. M., Ramadan, R. A., & Khedr, A. Y. (2016). Language and security for none english speakers. *International Journal of Computer Science and Information Security, 14*, 636-644

Andrade, A. D. (2009). Interpretive research aiming at theory building: Adopting and adapting the case study design. *Qualitative Report*, 14, 42-60.

Andraski, M. P., Chandler, C., Powell, B., Humes, D., & Wakefield, S. (2014). Bridging the divide: HIV prevention research and black men who have sex with men. *American Journal of Public Health*, *104*, 708-714. doi:10.2105/ajph.2013.301653

Andrikopoulos, V., Binz, T., Leymann, F., & Strauch, S. (2013). How to adapt applications for the Cloud environment. *Computing,* 95, 493-535. doi:10.1007/s00607-012-0248-2

Archambault, P. M., Thanh, J., Blouin, D., Gagnon, S., Poitras, J., Fountain, R., Légaré, F. (2015). Emergency medicine residents' beliefs about contributing to an online collaborative slideshow. CJEM : *Journal of the Canadian Association of Emergency Physicians*, 17, 374-386. doi: 10.1017/cem.2014.4

Ashraf, A., Narongsak, T., & Seigyoung A .(2014). The application of the technology acceptance model under different cultural contexts: The case of online shopping adoption." *Journal of International Marketing 22*, 68-93. doi:10.1509/jim.14.0065

Ajzen, I., & Fishbein, M. (1975). Belief, attitude, intention and behavior: An introduction to theory and research. Contemporary Sociology, 6, 244. doi:10.2307/2065853

Anyan, F. (2013). The influence of power shifts in data collection and analysis stages: A

focus on qualitative research interview. Qualitative Report, 18, 19.

Asiimwe, E. N., & Grönlund, A. (2015). MLCMS actual use, perceived use, and experiences of use. *International Journal of Education and Development using Information and Communication Technology*, *11*(1), 101A.

Avram, M. G. (2014). Advantages and challenges of adopting cloud computing from an enterprise perspective. *Procedia Technology*, 12, 529534. doi:10.1016/j.protcy.2013.12.525

Avvi Yucel, U & Gulbahar, Y. (2013). technology acceptance model: A Review of the Prior Predictors. *Journal Of Faculty Of Educational Sciences*, 46(1), 89-109. doi:10.1501/egifak_0000001275

Babbie, E. (2010). The Practice of Social Research Wadsworth Cengage Learning. *International Edition*.

Bailey, L. (2014). The origin and success of qualitative research. *International Journal of Market Research*, 56, 167-181. doi:10.2501/ijmr-2014-013

Balavivekanandhan, A., & Arulchelvan, S. (2015). A Study on Students Acquisition of IT Knowledge and Its Implication on M-Learning. *The Scientific World Journal*, 2015, 1–11. doi:10.1155/2015/248760

Berger, R. (2013). Now I see it, now I don't: Researcher's position and reflexivity in qualitative research. Qualitative Research, 15, 1-16. doi:10.1177/1468794112468475

Bernik, I., & Prislan, K. (2016). Measuring information security performance with 10 by 10 model for holistic state evaluation. *PLoS One, 11*, doi:10.1371/journal.pone.0163050

Bethencourt, J., Sahai, A., & Waters, B. (2007). Ciphertext-Policy Attribute-Based Encryption. *2007 IEEE Symposium on Security and Privacy (SP'07).* doi:10.1109/sp.2007.11

Bevan, M. T. (2014). A method of phenomenological interviewing. Qualitative Health Research, 24, 136-144. doi:10.1177/1049732313519710

Birt, L., Scott, S., Cavers, D., Campbell, C., & Walter, F. (2016). Member Checking. Qualitative Health Research, 26(13), 1802–1811. doi:10.1177/1049732316654870

Bogart, V. D., & Wichadee, S. (2015). Exploring students' intention to use LINE for academic purposes based on technology acceptance model. *International Review of Research in Open and Distance Learning*, 16. doi:10.19173/irrodl.v16i3.1894

Brakewood, B., & Poldrack, R. A. (2013). The ethics of secondary data analysis: Considering the application of Belmont principles to the sharing of neuroimaging data. *NeuroImage*, *82*, 671–676. doi:10.1016/j.neuroimage.2013.02.040

Bruner, G. C., & Kumar, A. (2005). Explaining consumer acceptance of handheld Internet devices. *Journal of business research*, 58, 553-558. doi:10.1016/j.jbusres.2003.08.002

Bryde, D., Broquetas, M., & Volm, J. M. (2013). The project benefits of building information modeling (BIM). International Journal of Project Management, 31,

971-980. doi:10.1016/j.ijproman.2012.12.001

Buschman, C. (2014). *A total cost matrix analysis and the impact of international supplier management* (Doctoral dissertation). Available from ProQuest Dissertations & Theses database. (UMI No. 1617454817)

Cabral, B. J. (2016). Exploring factors influencing information technology portfolio selection process in government-funded bioinformatics projects (Order No. 10241397).

Carter, N., Bryant-Lukosius, D., DiCenso, A., Blythe, J., & Neville, A. J. (2014). The use of triangulation in qualitative research. In *Oncology Nursing Forum, 41*, 545-547. doi:10.1188/14.ONF.545-547

Castillo-Montoya, M. (2016). Preparing for interview research: The interview protocol refinement framework. *The Qualitative Report, 21*, 811-830

Cayirci, E., Garaga, A., Oliveira, S. D., & Roudier, Y. (2016). A risk assessment model for selecting cloud service providers. *Journal of Cloud Computing, 5*(1), 1-12. doi:10.1186/s13677-016-0064-x

Charlebois, K., Palmour, N., & Knoppers, B. M. (2016). The adoption of cloud computing in the field of genomics research: The influence of ethical and legal issues. *PLoS One, 11.* doi:10.1371/journal.pone.0164347

Chi-Lun, L. (2014). The effects of ontology-based and password-protected blog access control on perceived privacy benefit and perceived ease of use. *Kybernetes*, 43, 325-340. doi:10.1108/K-12-2013-026

Christensen, C. M. (2011). *The innovator's dilemma: The revolutionary book that will*

change the way you do Business. New York, NY: HarperBusiness.

Chau, P.Y.K. (1996) "An empirical assessment of a modified technology acceptance model", Journal of Management Information Systems, 13, 185-204. doi:10.1080/07421222.1996.11518128

Chou, T. S. (2013). Security threats on cloud computing vulnerabilities. *International Journal of Computer Science & Information Technology*, 5, 79. doi:10.5121/ijcsit.2013.5306

Chou, C. H., Wang, Y. S., & Tang, T. I. (2015). Exploring the determinants of knowledge adoption in virtual communities: A social influence perspective. *International Journal of Information Management*, *35*, 364-376. doi:10.1016/j.ijinfomgt.2015.02.001

Cooper, Jeffrey A,M.D., M.M.M., Borasky, D., M.P.H., Rosenfeld, Stephen,M.D., M.B.A., & Sugarman, Jeremy, MD,M.P.H., M.A. (2016). Challenges in the ethical review of research involving complementary and integrative medicine. *Therapeutic Innovation & Regulatory Science, 50*, 337-341. doi:10.1177/2168479015620246

Cseko, G. C., & Tremaine, W. J. (2013). The role of the institutional review board in the oversight of the ethical aspects of human studies research. *Nutrition in Clinical Practice, 28*, 177–181. doi:10.1177/0884533612474042

Culbertson, S. S., Weyhrauch, W. S., & Huffcutt, A. I. (2017). A tale of two formats: Direct comparison of matching situational and behavior description interview questions. Human Resource Management Review, 27(1), 167-177.

Cunha, J. M., & Miller, T. (2014). Measuring value-added in higher education: Possibilities and limitations in the use of administrative data. *Economics of Education Review, 42*, 64-77. doi:10.1016/j.econedurev.2014.06.001

Daigneault, P. M., & Jacob, S. (2013). Unexpected but most welcome mixed methods for the validation and revision of the participatory evaluation measurement instrument. *Journal of Mixed Methods Research*, *8*(1), 6-24. doi:10.1177/1558689813486190

Da Veiga, A. (2016). Comparing the information security culture of employees who had read the information security policy and those who had not. *Information and Computer Security, 24*(2), 139-151. doi:10.1108/ics-12-2015-0048

Dean, J. (2014). Personal protective equipment: An antecedant to safe behavior? *Professional Safety*, 59, 41-46.

Davis Jr, F. D. (1986). A technology acceptance model for empirically testing new end-user information systems: *Theory and results* (Doctoral dissertation, Massachusetts Institute of Technology).

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS quarterly*, 319-340. doi:10.2307/249008

Davis, F., Bagozzi R., & Warshaw, P. (1989), User acceptance of computer technology: a comparison of two theoretical models," *Management Science*, 35, 982–1132. doi:10.1287/mnsc.35.8.982

Dey, B. L. (2013). A qualitative enquiry into technology acceptance and appropriation: A case study of Bangladeshi farmers' use of mobile telephony. Journal of Customer Behaviour, 12, 261-280. doi:10.1362/147539213x13832198705017

DiCicco-Bloom, B., & Crabtree, B. F. (2006). The qualitative research interview. *Medical Education*, 40, 314–321. doi:10.1111/j.1365-2929.2006.02418.x

Donald, A. C., Oli, S. A., & Arockiam, L. (2013). Mobile cloud security issues and challenges: A perspective. *International Journal of Electronics and Information Technology (IJEIT), ISSN*, 2277-3754.

Dove, E. S., Joly, Y., Tassé, A. M., Burton, P., Chisholm, R., Fortier, I & Kent, A. (2014). Genomic cloud computing: legal and ethical points to consider. *European Journal of Human Genetics*. 23, 1271–1278. doi:10.1038/ejhg.2014.196

Ebrahim, N. A. (2016). Promote and Enhance your Research through Linkedin. *Research Visibility and Impact-Repository*, 1(1), 1-36.

Esmaeilzadeh, P., Sambasivan, M., & Nezakati, H. (2014). The limitations of using the existing TAM in adoption of clinical decision support system in hospitals: An empirical study in malaysia. *International Journal of Research in Business and Social Science*, 3, 56-68.

Farkas, D., & Orosz, G. (2013). The link between ego-resiliency and changes in Big Five traits after decision making: The case of extraversion. *Personality and Individual Differences*, *55*, 440-445. doi:10.1016/j.paid.2013.04.003

Fateminezhad, A., & Soltanaghaei, M. R. (2016). An overview of cloud computing and its related security issues. Journal of Current Research in Science, (1), 410-414

Fernandez, A., del Rio, S., Lopez, V., Bawakid, A., del Jesus, M. J., Benítez, J. M., & Herrera, F. (2014). Big Data with Cloud Computing: an insight on the computing environment, MapReduce, and programming frameworks. Wiley Interdisciplinary Reviews: *Data Mining and Knowledge Discovery*, 4, 380-409.

Fowler, F. J., Jr. (2013). Survey research methods. Thousand Oaks, CA: Sage.

Foss, N. J., & Hallberg, N. L. (2014). How symmetrical assumptions advance strategic management research. Strategic Management Journal, 35, 903-913. doi:10.1002/smj.2130

Fusch, P. I., & Ness, L. R. (2015). Are we there yet? Data saturation in qualitative research. *The Qualitative Report*, *20*, 1408–1416.

Ghazizadeh, E., Zamani, M., Ab Manan, J., & Alizadeh, M. (2014). Trusted Computing Strengthens Cloud Authentication. The Scientific World Journal, 2014, 1–17. doi:10.1155/2014/260187

Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2013). Seeking qualitative rigor in inductive research notes on the Gioia methodology. *Organizational Research Methods*, 16(1), 15-31. doi:10.1177/1094428112452151

Goertz, G., & Mahoney, J. (2013). Methodological Rorschach tests: Contrasting interpretations in qualitative and quantitative research. Comparative Political Studies, 46, 236 –251. doi:10.1177/0010414012466376

Grossoehme, D. H. (2014). Overview of qualitative research. *Journal of health care chaplaincy*, 20, 109-122. doi:10.1080/08854726.2014.925660

Grossoehme, D. H., Cotton, S., Ragsdale, J., Quittner, A. L., McPhail, G., & Seid, M. (2013). "I honestly believe God keeps me healthy so I can take care of my child": Parental use of faith related to treatment adherence. *Journal of health care chaplaincy*, 19, 66-78. doi:10.1080/08854726.2013.779540

Guetterman, T. C. (2015). Descriptions of sampling practices within five approaches to qualitative research in education and the health sciences. Forum: *Qualitative Social Research*, 16(2), 1-23

Habjan, K. B., & Pucihar, A. (2017). The importance of business model factors for cloud computing adoption: Role of previous experiences. *Organizacija, 50*, 255-272. doi:10.1515/orga-2017-0013

Hankins, M., French, D., & Horne, R. (2000). Statistical guidelines for studies of the theory of reasoned action and the theory of planned behaviour. *Psychology and Health*, 15, 151-161. doi:10.1080/08870440008400297

Hess, T. J., McNab, A. L., & Basoglu, K. A. (2014). Reliability Generalization of Perceived Ease of Use, Perceived Usefulness, and Behavioral Intentions. *Mis Quarterly*, *38*, 1-28.

Hoffman, D., & Tarawalley, M. (2014). Frontline collaborations: The research relationship in unstable places. *Ethnography*, 15, 291–310. doi:10.1177/1466138114533463

Houghton, C., Casey, D., Shaw, D., & Murphy, K. (2013). Rigour in qualitative casestudy research. Nurse Researcher, 20, 1217. doi:10.7748/nr2013.03.20.4.12.e326

Hsu, C., Lee, M., & Su, C. (2013). The role of privacy protection in healthcare information systems adoption. *Journal of Medical Systems*, 37(5), 1-9966. doi:10.1007/s10916-013-9966-z

Huang, E. (2005). The acceptance of women-centric websites. *Journal of Computer Information Systems*, *45*, 75-83

Hung, C. N., Hwang, M. D., & Liu, Y. C. (2013). Show the way to information security governance for universities in taiwan. *Applied Mechanics and Materials, 278-280*, 2199. doi:10.4028/www.scientific.net/amm.278-280.2199

Inan, F. A., Namin, A. S., Pogrund, R. L., & Jones, K. S. (2016). Internet use and cybersecurity concerns of individuals with visual impairments. *Journal of Educational Technology & Society*, 19(1), 28-40.

Iqbal, S., & Bhatti, Z. A. (2015). An Investigation of University Student Readiness toward M-learning using technology acceptance model. The International Review of Research in Open and Distributed Learning, 16. doi:10.19173/irrodl.v16i4.2351

Irvine, A., Drew, P., & Sainsbury, R. (2013). Am I not answering your questions properly? Clarification, adequacy and responsiveness in semi-structured telephone and face-to-face interviews. *Qualitative Research*, *13*, 87-106. doi:10.1177/1468794112439086

Jacobson, R. M., Hanson, W. E., & Zhou, H. (2015). Canadian psychologists' test feedback training and practice: A national survey. *Canadian Psychology*, 56, 394-404.

Johnson, B. (2014). Ethical issues in shadowing research. Qualitative Research in Organizations and Management, 9, 21-40. doi:10.1108/QROM-09-2012-1099

Johnson, J. R. (2013). Counterfeit compliance with the HIPAA security rule: A study of information system success (Order No. 3594687).

Joo, Y. J., Joung, S., Lim, E., & Lee, M. (2015). Analysis of factors influencing facebook persistence. International Journal of Innovation, *Management and Technology*, 6, 105-108. doi:10.7763/IJIMT.2015.V6.583

Joslin, R., & Müller, R. (2016). Identifying interesting project phenomena using philosophical and methodological triangulation. *International Journal of Project Management*, 34, 1043-1056. doi:10.1016/j.ijproman.2016.05.005

Juels, A., & Oprea, A. (2013). New approaches to security and availability for cloud data. *Communications of the ACM*, 56, 6473. doi:10.1145/2408776.2408793

Kafle, N. P. (2013). Hermeneutic phenomenological research method simplified. Bodhi: *An Interdisciplinary Journal*, 5, 181-200. doi:10.3126/bodhi.v5i1.8053

Kalloniatis, C., Mouratidis, H., & Islam, S. (2013). Evaluating cloud deployment scenarios based on security and privacy requirements. *Requirements Engineering,* 18, 299-319. doi:10.1007/s00766-013-0166-7

Koufaris, M. (2002). Applying the technology acceptance model and flow theory to online consumer behavior. *Information systems research*, 13, 205-223. doi:10.1287/isre.13.2.205.83

Keith, M., Shao, B., & Steinbart, P. (2009). A behavioral analysis of passphrase design and effectiveness. Journal of the Association for Information Systems, 10, 63-89.

Khan, S. N. (2014). Qualitative research method: Phenomenology. *Asian Social Science*, *10*, 298–310. doi:10.5539/ass.v10n21p298

Kharaji, M. Y., & Rizi, F. S. (2014). A fast survey focused on methods for classifying anonymity requirements. *International Journal of Computer Science and Information Security*, 12, 59-63

Khosravan, S., Mazlom, B., Abdollahzade, N., Jamali, Z., & Mansoorian, M. R. (2014). Family participation in the nursing care of the hospitalized patients. *Iranian Red Crescent Medical Journal*, 16(1), 1-6. doi:10.5812/ircmj.12868

Kim, E. B. (2013). Information Security Awareness Status of Business College: Undergraduate Students. *Information Security Journal: A Global Perspective*, 22, 171–179. doi:10.1080/19393555.2013.828803

Kipo, D. (2013). Mixed research methods: Reflections on social public policy. *Asian Social Science*, 9, 259-268. doi:10.5539/ass.v9n17p259

Kreutz, D., Esteves-Verissimo, P., Magalhaes, C., & Ramos, F. (2017). The KISS principle in Software-Defined Networking: An architecture for Keeping It Simple and Secure. *arXiv preprint arXiv:1702.04294*.

Kshetri, N. (2013). Privacy and security issues in cloud computing: The role of institutions and institutional evolution. *Telecommunications Policy*, 37, 372-386. doi:10.1016/j.telpol.2012.04.011

Kumar, V., Jain, A., & Barwal, P. N. (2014). Wireless sensor networks: security issues, challenges and solutions. International Journal of Information and Computation Technology, 4, 859-868.

Lai, I. K. W., Tam, S. K. T., & Chan, M. F. S. (2012). Knowledge cloud system for network collaboration: A case study in medical service industry in China. *Expert Systems with Applications, 39*, 11801–12290. doi:10.1016/j.eswa.2012.04.057

Lambert, V., Glacken, M., & McCarron, M. (2013). Meeting the information needs of children in hospital. *Journal of Child Health Care*, 17, 338-353 doi:10.1177/1367493512462155

Langen, T. A., Mourad, T., Grant, B. W., Gram, W. K., Abraham, B. J., Fernandez, D. S., & Hampton, S. E. (2014). Using large public datasets in ecology classroom. Frontiers in Ecology and the Environment, 12, 362-363. doi:10.1890/1540-9295-12.6.362

Lee, D. T., Woo, J., & Mackenzie, A. E. (2002). The cultural context of adjusting to nursing home life Chinese elders' perspectives. *The Gerontologist*, 42, 667-675.

Leedy, P. D., & Ormrod, J. E. (2010). Practical research: Planning and design (9th ed.), Upper Saddle River, New Jersey: Pearson Education Inc.

Leedy, P. D., & Ormrod, J. E. (2015). Practical research: Planning and design (9th ed.). Upper Saddle River, NJ: Merrill Prentice-Hall

Legris, P., Ingham, J. & Collerette, P. (2003). Why do people use information technology? A critical review of the technology acceptance model. *Information & Management, 40*, 191–204. doi:10.1016/s0378-7206(01)00143-4

Levy, M. (2015). The role of qualitative approaches to research in CALL contexts: Closing in on the learner's experience. *CALICO Journal*, 32, 554-568. doi:10.1558/cj.v32i3.26620

Liaw, S.-S., & Huang, H.-M. (2015). How factors of personal attitudes and learning environments affect gender difference toward mobile learning acceptance. *The International Review of Research in Open and Distributed Learning, 16*. doi:10.19173/irrodl.v16i4.2355

Loh, J. (2013). Inquiry into Issues of Trustworthiness and Quality in Narrative Studies: A Perspective. *The Qualitative Report*, 18(33), 1-15.

Liu, C. H., Tang, W. R., Wang, H. M., & Lee, K. C. (2013). How cancer patients build trust in traditional Chinese medicine. *European Journal of Integrative Medicine*, *5*, 495-500. doi:10.1016/j.eujim.2013.08.003

Lu, L. C., Chang, H. H., & Yu, S. T. (2013). Online shoppers' perceptions of e-retailers' ethics, cultural orientation, and loyalty: An exploratory study in Taiwan. *Internet Research*, *23*, 47-68. doi:10.1108/10662241311295773

Lu, J., Liu, C., Yu, C. S., & Yao, J. E. (2014). Exploring factors associated with wireless internet via mobile technology acceptance in Mainland China.*Communications of the IIMA*, *3*, 9.

Lucas, S. R. (2014). Beyond the existence proof: Ontological conditions, epistemological implications, and in-depth interview research. *Quality and Quantity, 48*(1), 387-408. doi:10.1007/s11135-012-9775-3

Mangioni, V., & McKerchar, M. (2013). Strengthening the validity and reliability of the Focus group as a method in tax research. e*Journal of Tax Research*, *11*, 176-190.

Mao-Yu, Z., Li, J., Hu, H., & Yi-Tao, W. (2015). Seizing the strategic opportunities of emerging technologies by building up innovation system: Monoclonal antibody

development in china. *Health Research Policy and Systems, 13. doi:10.1186/s12961-015-0056-1*

Marshall, C., & Rossman, G. (2016). *Designing qualitative research* (6th ed.). Thousand Oaks, CA: Sage.

Mathieson, K. (1991). Predicting user intentions: comparing the technology acceptance model with the theory of planned behavior. *Information systems research*, 2, 173-191. doi:10.1287/isre.2.3.173

Matrane, O., Talea, A., Okar, C., & Talea, M. (2015). Towards A new maturity model for information system. *International Journal of Computer Science Issues (IJCSI), 12*, 268-275.

McCusker, K., & Gunaydin, S. (2015). Research using qualitative, quantitative or mixed methods and choice based on the research. *Perfusion,* 30, 537-542. doi:10.1177/0267659114559116

McIntosh, L. (2017). Reducing technology costs for small real estate businesses by using cloud and mobility (Order No. 10265709).

McKelvey, B., & Pfeffer, J. (1984). Organizations and Organization Theory. Administrative Science Quarterly, 29, 640. doi:10.2307/2392948

Mishra, S. (2015). Organizational objectives for information security governance: A value focused assessment. *Information & Computer Security*, *23*, 122-144. doi:10.1108/ICS-02-2014-0016

Misenheimer, K. J. (2014). Exploring Information Technology Security Requirements for Academic Institutions to Reduce Information Security Attacks, Breaches, and Threats. NORTHCENTRAL UNIVERSITY.

Mishra, A., Mathur, R., Jain, S., & Rathore, J. S. (2013). Cloud computing security. *International Journal on Recent and Innovation Trends in Computing and Communication*, *1*, 36-39.

Mohammadi, H. (2015). A study of mobile banking usage in iran. *The International Journal of Bank Marketing, 33*(6), 733-759. doi:10.1108/ijbm-08-2014-0114

Mosse, D. (2015). Misunderstood, misrepresented, contested?: Anthropological knowledge production in question. *Focaal,* 2015 128-137. doi:10.3167/fcl.2015.720111

Naik, N., & Jenkins, P. (2016, March). A secure mobile cloud identity: Criteria for effective identity and access management standards. In *Mobile Cloud Computing, Services, and Engineering (MobileCloud), 2016 4th IEEE International Conference on* (pp. 89-90). IEEE. doi:10.1109/mobilecloud.2016.22

National Commission for the Protection of Human Subjects of Biome Beha Resea, & Ryan, K. J. P. (1978). The Belmont Report: Ethical Principles and Guidelines for the Protection of Human Subjects of Research-the National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. US Government Printing Office.

Nielsen, R. B. (2011). Cues to quality in quantitative research papers. *Family and Consumer Sciences Research Journal*, *40*(1), 85-89 doi:10.1111/j.1552-

3934.2011.02090.x

Ngoqo, B., & Flowerday, S. V. (2015). Exploring the relationship between student mobile information security awareness and behavioural intent. *Information and Computer Security*, 23, 406-420. doi:10.1108/ics-10-2014-0072

Nicho, M., & Hendy, M. (2013). Dimensions Of Security Threats In Cloud Computing: A Case Study. *Review of Business Information Systems (RBIS*), 17, 159. doi:10.19030/rbis.v17i4.8238

Noble, H., & Smith, J. (2015). Issues of validity and reliability in qualitative research. *Evidence Based Nursing*, 18, 34–35. doi:10.1136/eb-2015-102054

Okantey, M., & Addo, H. H. (2016). Effect of theoretical and institutional factors on the adoption of E-learning. *European Scientific Journal*, 12, doi:10.19044/esj.2016.v12n16p475

Okundaye, K. E. (2016). *Adoption of Information and Communication Technology in Nigerian Small-to Medium-Size Enterprises (Doctoral dissertation, Walden University).*

Onwuegbuzie, A. J., Frels, R. K., & Hwang, E. (2016). Mapping Saldaňa's coding methods onto the literature review process. *Journal of Educational Issues, 2*, 130-150. doi:10.5296/jei.v2i1.8931

Opitz, D., & Witzel, A. (2005). The concept and architecture of the bremen life course archive. *Forum: Qualitative Social Research, 6*(2)

Osho, O., & Onoja, A. D. (2015). National cyber security policy and strategy of nigeria: A qualitative analysis. *International Journal of Cyber Criminology, 9*(1), 120-143.

Park, E., & Kim, K. J. (2014). An Integrated Adoption Model of Mobile Cloud Services: Exploration of Key Determinants and Extension of technology acceptance model. Telematics and Informatics, 31, 376–385. doi:10.1016/j.tele.2013.11.008

Peiris, P. M., Kulkarni, D., & de Silva Mawatha, C. R. (2015). Implications of Trust and Usability on E-Commerce Adoption. *International Journal of Business and Information*, *10*, 519.

Peñaloza-Salazar C., Gutiérrez-Maldonado J., Ferrer-García M., et al. (2015). Cognitive mechanisms underlying Armoni, A computer-assisted cognitive training programme for individuals with intellectual disabilities. *Anales de Psicología/ Annals of Psychology*, 32(1), 115-124. doi:10.6018/analesps.32.1.194511

Peredaryenko, M. S., & Krauss, S. E. (2013). Calibrating the human instrument: Understanding the interviewing experience of novice qualitative researchers. *Qualitative Report, 18*, 1-17.

Persico, D., Manca, S., & Pozzi, F. (2014). Adapting the technology acceptance model to evaluate the innovative potential of e-learning systems. Computers in Human Behavior, 30, 614-622. doi:10.1016/j.chb.2013.07.045

Peterlongo, G., Ionescu, S., & Gavrila, L. (2015). Informational signals. *FAIMA Business & Management Journal, 3*, 19-30.

Pogrund, R. L., Darst, S., & Munro, M. P. (2015). Initial validation study for a scale used to determine service intensity for itinerant teachers of students with visual impairments. *Journal of Visual Impairment & Blindness (Online),* 109, 433.

Radner, R., & Rothschild, M. (1975). On the allocation of effort. Journal of Economic Theory, 10, 358–376. doi:10.1016/0022-0531(75)90006-x

Ranjith, G., Vijayachandra, J., Sagarika, P., & Prathusha, B. (2015). Intelligence based authentication – Authorization and auditing for secured data storage. *International Journal of Advances in Engineering & Technology, 8*, 628-636.

Ratten, V. (2015). A cross-cultural comparison of online behavioural advertising knowledge, online privacy concerns and social networking using the technology acceptance model and social cognitive theory. *Journal of Science and Technology Policy Management, 6*(1), 25-36. doi:10.1108/jstpm-06-2014-0029

Ray, D. (2016). Cloud adoption decisions: Benefitting from an integrated perspective. *Electronic Journal of Information Systems Evaluation, 19*(1), 3-22.

Reid, S., & Mash, B. (2014). African Primary Care Research: Qualitative interviewing in primary care. *Afr J Prim Health Care Fam Med*, 6, 1-6. doi:10.4102/phcfm.v6i1.632

Revoredo da Silva, C. M., Costa da Silva, J. L., Rodrigues, R. B., Medeiros Campos, G. M., Marques do Nascimento, L., & Cardoso Garcia, V. (2013). Security Threats in Cloud Computing Models: Domains and Proposals. *2013 IEEE Sixth International Conference on Cloud Computing*. doi:10.1109/cloud.2013.125

Richards, K. (2003). Qualitative inquiry in TESOL. Springer.

Richardson, F.W. (2014). *Enhancing strategies to improve workplace performance* (Doctoral dissertation). Available from ProQuest Dissertations and Theses database. (UMI No. 3669117)

Risk, J. L. (2013). Building a new life: A chaplain's theory based case study of chronic illness. *Journal of health care chaplaincy*, 19, 81-98. doi:10.1080/08854726.2013.806117

Rizvi, S. Z. R., & Fong, P. W. (2016, March). Interoperability of relationship-and role-based access control. In *Proceedings of the Sixth ACM Conference on Data and Application Security and Privacy* (pp. 231-242). ACM.

Robinson, O. C. (2014). Sampling in interview-based qualitative research: A theoretical and practical guide. *Qualitative Research in Psychology*, 11, 25-41. doi:10.1080/14780887.2013.801543

Rogers, W., & Lange, M. M. (2013). Rethinking the vulnerability of minority populations in research. *American Journal of Public Health*, *103*, 2141–2146. doi:10.2105/ajph.2012.301200

Rogers, A. D. (2016). *Examining small business adoption of computerized accounting systems using the technology acceptance model* (Order No. 10001635).

Rong, C., Nguyen, S. T., & Jaatun, M. G. (2013). Beyond lightning: A survey on security challenges in cloud computing. *Computers & Electrical Engineering,* 39(1), 47-54. doi:10.1016/j.compeleceng.2012.04.015

Roulston, K. & Shelton, S. A. (2015). Reconceptualizing bias in teaching qualitative research methods. *Sage Journals*, *21*, 332-342. doi:10.1177/1077800414563803

Rutter, D. R., & Bunce, D. J. (1989). The theory of reasoned action of Fishbein and Ajzen: A test of Towriss's amended procedure for measuring beliefs. *British Journal of Social Psychology*, *28*(1), 39-46. doi:10.1111/j.2044-8309.1989.tb00844.x

Salas, A., & Moller, L. (2015). The value of voice thread in online learning: Faculty perceptions of usefulness. *Quarterly Review of Distance Education*, 16(1), 11-24,75-76

Sampson, J. P., Hou, P.-C., Kronholz, J. F., Dozier, V. C., McClain, M.-C., Buzzetta, M., … Kennelly, E. L. (2014). A content analysis of career development theory, research, and practice-2013. *The Career Development Quarterly*, *62*, 290–326. doi:10.1002/j.2161-0045.2014.00085.x

Sareen, P. (2013). Cloud computing: types, architecture, applications, concerns, virtualization and role of it governance in cloud. *International Journal of Advanced Research in Computer Science and Software Engineering*, *3(3)*.

Sauls, J., & Gudigantala, N. (2013). Preparing information systems (IS) graduates to meet the challenges of global IT security: *Journal of Information Systems Education*, 24, 71–73.

Scholtz, B., & Kapeso, M. (2014). An m-learning framework for ERP systems in higher education. Interactive *Technology and Smart Education*, 11, 287. doi:10.1108/itse-09-2014-0030

Schoonenboom, J. (2014). Using an adapted, task-level technology acceptance model to explain why instructors in higher education intend to use some learning

management system tools more than others. Computers & Education, 71, 247-256. doi:10.1016/j.compedu.2013.09.016

Sen, J. (2013). Security and Privacy Issues in Cloud Computing. *Cloud Technology*, 1585–1630. doi:10.4018/978-1-4666-6539-2.ch074

Shah, M. H., Peikari, H. R., & Yasin, N. M. (2014). The determinants of individuals' perceived e-security: Evidence from Malaysia. International Journal of Information Management, 34(1), 48–57. doi:10.1016/j.ijinfomgt.2013.10.001

Sharma, S. K., Al-Badi, A. H., Govindaluri, S. M., & Al-Kharusi, M. H. (2016). Predicting motivators of cloud computing adoption: A developing country perspective. Computers in Human Behavior, 6261-6269. doi:10.1016/j.chb.2016.03.073

Sharma, S., Gupta, G., & Laxmi, P. R. (2014). A survey on cloud security issues and techniques. International Journal on Computational Science & Applications, 4(1), 125–132. doi:10.5121/ijcsa.2014.4112

Shaw, Simuel, I.,II. (2015). A business integration model for the adaptation of biometrics technology in the 21st century (Order No. 3733494).

Sheppard B, Hartwick J, Warshaw P. (1988) The Theory of Reasoned Action: A Meta-Analysis of Past Research with Recommendations for Modifications and Future Research. *Journal Of Consumer Research,* 15:325-343. doi:10.1086/209170

Sikweyiya, Y., & Jewkes, R. (2013). Potential motivations for and perceived risks in research participation: Ethics in health research. *Qualitative Health Research*, *23*, 999-1009. doi:10.1177/1049732313490076

Singh, V., & Pandey, S. K. (2013). Cloud Security Related Threats. *International Journal of Scientific & Engineering Research*, 4, 2571.

Srinivasan, S. (2013). Is security realistic in cloud computing? *Journal of International Technology and Information Management, 22*, 47-66.

Stanciu, V., & Tinca, A. (2016). Students' awareness on information security between own perception and reality – an empirical study. *Accounting & Management Information Systems / Contabilitate Si Informatica De Gestiune*, 15, 112-130.

Stoetzer, O. R. (2016). You are your password: IT and public safety personnel's views of biometrics as identity and access management on college campuses (Order No. 10130912).

Straub, D., Keil, M. & Brenner, W. (1997) Testing the technology acceptance model across cultures: a three country study." *Information & Management*, 33, 1-11. doi:10.1016/s0378-7206(97)00026-8

Svensson, L., & Doumas, K. (2013). Contextual and analytic: Qualities of research methods exemplified in research on teaching. *Qualitative Inquiry, 19*, 441-450. doi:10.1177/1077800413482097

Svilar, A., & Zupancic, J. (2016). User experience with security elements in internet and mobile banking. *Organizacija, 49*, 251-260. doi:10.1515/orga-2016-0022

Tai, L. (2015). The impact of corporate governance on the efficiency and financial performance of GCC National banks. *Middle East Journal of Business*, 10, 12-16, doi:10.5742/mejb.2015.92594

Thomas, M. V., Dhole, A., & Chandrasekaran, K. (2015). Single sign-on in cloud federation using CloudSim. *International Journal of Computer Network and Information Security, 7*, 50-58. doi:10.5815/ijcnis.2015.06.06

Tomkinson, S. (2014). Doing fieldwork on state organizations in democratic settings: Ethical issues of research in refugee decision making. *In Forum Qualitative Sozialforschung/Forum: Qualitative Social Research* 16,(1**)**

Trafimow, D. (2014). Considering quantitative and qualitative issues together. Qualitative Research in Psychology, 11(1), 15-24. doi:10.1080/14780887.2012.743202

Turgut, M. (2014). Development of the spatial ability self-report scale (SASRS): reliability and validity studies. *Qualitative and Quantitative Analysis in Social Science*, *49*, 1997-2014. doi:10.1007/s11135-014-0086-8

Underhill, K. (2014). Legal and ethical values in the resolution of research-related disputes: How can IRBs respond to participant complaints? *Journal of Empirical Research on Human Research Ethics*, 9, 71–82. doi:10.1525/jer.2014.9.1.71

van Dijk, H., Fischer, A. R., Marvin, H. J., & van Trijp, H. C. (2017). Determinants of stakeholders' attitudes toward a new technology: nanotechnology applications for food, water, energy and medicine. *Journal Of Risk Research*, 20, 277-298. doi:10.1080/13669877.2015.1057198

Venkatesh, V., Brown, S. A., & Bala, H. (2013). Bridging the Qualitative-Quantitative Divide: Guidelines for conducting mixed methods research in information systems. *MIS quarterly,* 37, 21-54.

Wakefield, A. (2015). Synthesising the literature as part of a literature review. *Nursing Standard* (2014+), 29, 44. doi:10.7748/ns.29.29.44.e895

Wara, Y. M., & Singh, D. (2015). A guide to establishing computer security incident response team (CSIRT) for national research and education network (NREN). *African Journal of Computing & ICT*, *8*, 1-8.

Wei, L., Zhu, H., Cao, Z., Dong, X., Jia, W., Chen, Y., & Vasilakos, A. V. (2014). Security and privacy for storage and computation in cloud computing. *Information Sciences*, *258*, 371-386. doi:10.1016/j.ins.2013.04.028

White, J., & Drew, S. (2011). Collecting data or creating meaning? *Qualitative Research Journal, 11*, 3–12. doi:10.3316/QRJ1101003

Whiting, L. S. (2008). Semi-structured interviews: guidance for novice researchers. *Nursing Standard*, 22, 35–40. doi:10.7748/ns2008.02.22.23.35.c6420

Whitman, M. E., & Mattord, H. J. (2014). Information Security Governance for the Non-Security Business Executive. *Journal of Executive Education*,*11*(1).

Widodo, H. P. (2014). Methodological considerations in interview data transcription. *International Journal of Innovation in English Language Teaching and Research*, 3, 101-107

Wong, S., & Cooper, P. (2016). Reliability and validity of the explanatory sequential design of mixed methods adopted to explore the influences on online learning in hong kong bilingual cyber higher education. *International Journal of Cyber Society and Education, 9*, 45-66. doi:10.7903/ijcse.1475

Yaokumah, W. (2014). Information security governance implementation within Ghanaian

industry sectors: An empirical study. *Information Management & Computer Security*, *22*, 235-250. doi:10.1108/IMCS-06-2013-0044

Yin, R. (1981). The Case Study Crisis: Some Answers. *Administrative Science Quarterly, 26*, 58-65. doi:10.2307/2392599.

Yin, R. K. (2014). Case study research: Design and methods. Thousand Oaks, CA: Sage

Zardari, A., Jung, L. T., & Zakaria, N. (2014). A quantitative analysis of cloud users' satisfaction and data security in cloud models. *Science and Information Conference*, 42-47. doi:10.1109/SAI.2014.6918170

Appendix A: Interview Questions

1. What strategies have you used to implement secure access methods to protect data on the cloud infrastructure?
2. What did you think was the deciding factors to implement the current security methods over other security methods there are available?
3. Was there any training that you obtained that aided in your decision to suggest the current security measure that is in place?
4. Were there any concerns that you had regarding the adoption of the current security method?
5. Did you face any barriers when trying to implement the security policy?
6. In what ways do you feel that the current security policy that is in place is more beneficial than the prior process?
7. How well do you think others have accepted the security policy when it was implemented?
8. What processes do you have in place for training employees with regards to security on the cloud?
9. Do you have anything else to add that I have not asked about security methods that you have implemented regarding the cloud?

Appendix B: Interview Protocol

Participant Number ___

Hello, Mr./Mrs./Ms. (name) My name is Eric Harmon. I want to thank you for agreeing to participate in my DIT study and allocating time from your busy schedule for me to conduct this interview.	As I have mentioned in the email and in the consent form that I have sent to you, my study relates to strategies used by cloud security managers to implement secure access methods to protect data on the cloud infrastructure. Do you still agree to participate in my study?
	If the participant wishes to no longer participate in the study make note of their decision and thank them for their time. If the participant agrees to participate, proceed with the interview questions.
• Look for any nonverbal queues • Since questions are open ended, identify any items that can be explored further • Paraphrase as needed	1. What strategies have you used to implement secure access methods to protect data on the cloud infrastructure? 2. What did you think was the deciding factors to implement the current security methods over other security methods there are available? 3. Was there any training that you obtained that aided in your decision

	to suggest the current security measure that is in place? 4. Were there any concerns that you had regarding the adoption of the current security method? 5. Did you face any barriers when trying to implement the security policy? 6. In what ways do you feel that the current security policy that is in place is more beneficial than the prior process? 7. How well do you think others have accepted the security policy when it was implemented? 8. What processes do you have in place for training employees with regards to security on the cloud? 9. Do you have anything else to add that I have not asked about security methods that you have

	implemented regarding the cloud?

Appendix D: Letter of Invitation

Dear Participant:

My name is Eric Harmon. I am currently pursuing a Doctorate of Information Technology (DIT) through Walden University in Minneapolis. My doctoral study project is to explore strategies used by cloud security managers to implement secure access methods to protect data on the cloud infrastructure.

I am interested in studying the strategies that security managers use to protect information that is stored on the cloud. Permission was granted to conduct interviews in your organization and the manager has forwarded this letter out on my behalf to all security managers who are 18 years of age or older. This letter of invitation is to all security managers who want to volunteer and participate in the below research study. The interviews will be held during a time and date that is convenient with you, as the participant.

The interview process may last approximately 60-120 minutes. Your protection in your participation and information will be consistent with Walden University's confidentiality guidelines. Your participation will be instrumental in providing the required data best to analyze strategies to strategies used by cloud security managers to implement secure access methods to protect data on the cloud infrastructure. If you decide to participate, I will give you the consent form for review and for signature prior to the start of the focus group. This will allow for any questions you might have prior to your signature. The consent form describes your rights during the process and the purpose of the doctoral study. At the end of this doctoral research study, I will share the results and findings with participants, scholars, and other stakeholders.

Interview participation will be voluntary. Everyone will respect your decision of whether or not you choose to be in the study. If you decide to join the study now, you can still change your mind later. You may stop at any time. All willing participants interested must give their names to their manager or email me directly confirming their acceptance to participate in the study. Please advise if you have any questions or require any additional information.

Thank you for your time and consideration,

Harmon Walden University DIT Student